SS2GD8I

6-port 10/100/1000 + 2 Combo-SFP Port

L2 Managed Switch

User's Guide

Version 1.0

Amer.com

6901 Bryan Dairy Road, Suite 150, Largo, FL 33777

© Amer.com Corp., 1997-2006 All rights reserved. No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Amer.com, as stipulated by the United States Copyright Act of 1976.

Amer.com reserves the right to make changes to this document and the products which it describes without notice. Amer.com shall not be liable for technical or editorial errors or omissions made herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

Amer.com is a registered trademark of Amer.com. All other trademarks and trade names are properties of their owners.

Table of Contents

1 INTRODUCTION 1

1.1 PRODUCT OVERVIEW 1
1.2 KEY FEATURES OF THE SWITCH 1
1.3 CHECKLIST 1
1.4 FEATURES 2
1.5 SS2GD8I DIAGRAM 3
1.5.1 Front Panel 3
1.5.2 Rear Panel 4
1.6 FIBER TRANSCEIVERS 4

2 INSTALLATION 5

2.1 INSTALLING SWITCH INTO 19-INCH RACK 5
2.2 CABLE INSTALLATION 5
2.2.1 Cabling Requirements 6
2.2.2 Configuring the Switch 9

3 WEB INTERFACE 11

3.1 HOME PAGE 12
3.1.1 System Information 13
3.1.2 IP Configuration 14
3.1.3 Time 15
3.1.4 Account Configuration 16
3.1.5 Management Policy 16
3.1.6 Virtual Stack 17
3.2 PORT CONFIGURATION 18
3.2.1 Port Status 18
3.2.2 Port Configuration 19
3.2.3 Simple Counter 20
3.2.4 Detail Counter 21
3.3 MIRROR 23
3.4 BANDWIDTH MANAGEMENT 24
3.5 QOS (QUALITY OF SERVICE) CONFIGURATION 25
3.6 SNMP CONFIGURATION 29
3.7 IGMP SNOOPING 30
3.8 MAXIMUM PACKET LENGTH 31
3.9 DHCP BOOT 32
3.10 VLAN 32
3.10.1 VLAN Mode 32
3.10.2 Tag-based Group 33
3.10.3 Port-based Group 34
3.10.4 Tag Rule 35
3.11 MAC TABLE 36
3.11.1 Information 37
3.11.2 Maintenance Page 38
3.11.3 Static Forward 38
3.11.4 Static Filter 39
3.11.5 MAC Alias 39
3.12 GVRP CONFIGURATION 40
3.12.1 Config 40
3.12.2 Counter 42
3.12.3 Information 42

3.13 STP CONFIGURATION 43
3.13.1 STP Status 43
3.13.2 Configuration 44
3.13.3 Port 45
3.14 TRUNKING CONFIGURATION 46
3.14.1 Port 47
3.14.2 Aggregator View 47
3.14.3 System Priority 48
3.15 802.1X CONFIGURATION 49
3.15.1 State 49
3.15.2 Mode 49
3.15.3 Security 50
3.16 ALARM CONFIGURATION 52
3.16.1 Events 52
3.16.2 Email/SMS 53
3.17 CONFIGURATION 54
3.17.1 Save/Restore 54
3.17.2 Config File 54
3.18 DIAGNOSTICS 55
3.18.1 Diagnostics 55
3.18.2 Loopback 56
3.18.3 Ping Test 56
3.19 TFTP SERVER 57
3.20 LOG 57
3.21 FIRMWARE UPGRADE 58
3.22 REBOOT 58
3.23 LOGOUT 59

4 CLI INTERFACE 60

4.1 CLI MANAGEMENT 60
4.1.1 Login 60
4.2 CLI COMMANDS 60
4.2.1 CLI Global Commands 61
4.2.2 Local Commands of CLI 65

5 TROUBLESHOOTING 126

5.1 RESOLVING CONNECTION PROBLEMS 126
5.2 Q&A 126

APPENDIX A: TECHNICAL SPECIFICATIONS 127

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4K V CD, 8KV, AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1KV – (power line), 0.5KV – (signal line)

About this user's manual

This user's manual will show you how to install and connect the switch to your network and also how to configure and monitor the switch through the built-in CLI and web interface through RS-232 serial interface and Ethernet with step-by-step instructions. Many explanations of hardware and software functions are shown as well as examples of the operation for the web-based graphical user interface (GUI) and command-line interface (CLI).

Overview of this user's manual

- Chapter 1 "Introduction" describes the features of 8 Gigabit L2 Managed Switch
- Chapter 2 "Installation"
- Chapter 3 "Operation of Web-based Management"
- Chapter 4 "Operation of CLI Management"
- Chapter 5 "Maintenance"

1 Introduction

1.1 Product Overview

The SS2GD8I is a managed switch that meets all IEEE802.3/u/x/z Fast Ethernet and Gigabit specifications. The switch features 6 Gigabit copper ports and 2 Gigabit Combo-SFP ports. The switch can be managed through the RS-232 serial port or through an Ethernet port using either the CLI or Web GUI. With an SNMP agent, the network administrator can also log into the switch to monitor, configure and control the switch using SNMP. In addition, the switch features comprehensive and useful functions such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON, and IGMP Snooping.

The 10/100/1000Mbps Ethernet ports are standard ports that meet all IEEE 802.3/u/x/z Fast Ethernet and Gigabit specifications. The 1000Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceivers are designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

1.2 Key Features of the Switch

QoS: Supports Quality of Service using the 802.1p standard. There are two priority queues and packet transmission schedules.

Spanning Tree: Supports 802.1D, 802.1w (RSTP, Rapid Spanning Tree Protocol) standards.

VLAN: Supports port-based VLAN and 802.1Q tagged VLAN. Supports 256 active VLANs and 4094 VLAN IDs.

Port Trunking: Supports static port trunking and port trunking with 802.3ad LACP.

Bandwidth Control: Supports ingress and egress per port bandwidth control.

Port Security: Supports allowing and denying forwarding and port security with MAC address.

SNMP/RMON: SNMP agent and RMON MIB. The SNMP agent is a software client which uses the SNMP protocol to receive commands from the SNMP manager on the server and return the corresponding data, i.e. MIB object. The SNMP agent will also actively issue TRAP information when events occur. RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.

The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757) - statistics groups 1, 2, 3, 9, Ethernet-like MIB (RFC 1643), Ethernet MIB (RFC 1643).

IGMP Snooping: Supports IGMP version 2 (RFC 2236). The IGMP snooping function is used to establish multicast groups to forward multicast packets to the member ports which avoid wasting the bandwidth when IP multicast packets are sent over the network.

1.3 Checklist

Before you start using the switch, verify that the package contains the following items:

- SS2GD8I
- User's Manual on CD-ROM
- AC Power Cord

- RS-232 Cable

Please notify your sales representative immediately if any of the aforementioned items are missing or damaged.

1.4 Features

The SS2GD8I switch provides the features listed below for users to perform system network administration and service the network efficiently and securely.

Hardware

- 6 10/100/1000Mbps Auto-negotiation Gigabit Ethernet ports
- 2 10/100/1000Mbps Combo-SFP ports
- 144KB on-chip frame buffer
- Jumbo frame support
- Programmable classifier for QoS (Layer 4/Multimedia)
- 8K MAC address and 4K VLAN support (IEEE802.1Q)
- Per-port shaping, policing, and Broadcast Storm Control
- 802.1Q Q-in-Q nested VLAN support
- Full-duplex flow control (IEEE 802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LEDs: Power, LINK/ACT and 10/100/1000Mbps for Ethernet Ports 1-8, LINK/ACT for SFP Ports 7, 8

Management

- Port configuration
- Per port traffic monitoring counters
- Port mirroring
- Static trunks
- 802.1Q VLAN
- Maximum packet length can be up to 9208 bytes for jumbo frames
- DHCP Broadcasting Suppression to avoid network crashes
- Sends trap events when monitored events occur
- Default configuration can be restored to overwrite the current configuration which is working on via web browser and CLI
- Hot-pluggable SFP modules
- Quality of Service (QoS) for real time applications based on Layer 2-4 information, such as VoIP
- Built-in web-based management and CLI management, providing a more convenient UI for the user
- Port mirroring with ingress traffic
- Rapid spanning tree (802.1w RSTP)
- 802.1x port security on a VLAN

- SNMP access can be disabled and prevent from unauthorized SNMP access
- Ingress, non-unicast and egress bandwidth rating management with a resolution of 1Mbps
- The trap event and alarm message can be sent via e-mail and mobile phone SMS
- Diagnostics to let administrators know the hardware status
- External loopback test to check if the link is ok
- TFTP for firmware upgrade, system log upload and config file import/export
- Remote boot the device through user interface and SNMP
- Network time synchronization and daylight saving time
- 120 event log records in the main memory and displayed on the local console

1.5 SS2GD8I Diagram

Figure 1-1: SS2GD8I

1.5.1 Front Panel

There are 8 Gigabit Ethernet ports and 2 SFP fiber ports for optional removable transceivers on the front of the switch. The LEDs located on the panel consists of a Power LED which indicates the power status and LEDs for each port on the switch.

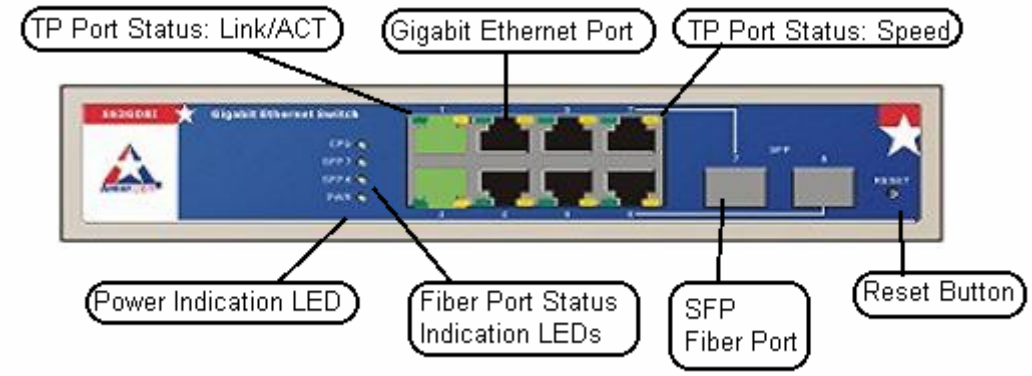

Figure 1-2: Front Panel

LED Indicators

POWER: Lights up green when switch is receiving power.

CPU: Lights up green when switch is on, flashes when CPU is working.

LINK/ACT: Lights up green when connected to a device, flashes when transmitting data.

10/100/1000Mbps: Lights up green when connected at 1000Mbps, amber when connected at 100Mbps, and is off when connected at 10Mbps or not connected.

SFP: Lights up green when connected to a device, blinks when transmitting data.

1.5.2 Rear Panel

The RS-232 port used for command line management and the power outlet are on the rear of the unit.

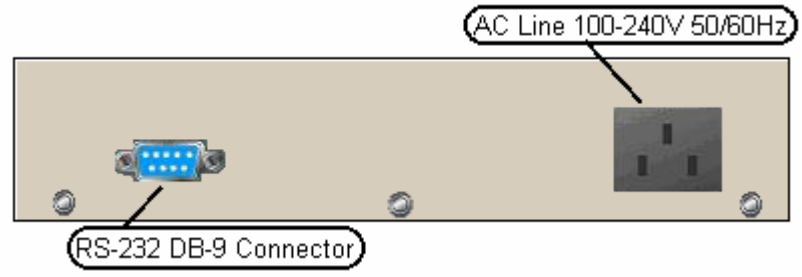

Figure 1-3: Rear Panel

1.6 Fiber Transceivers

Ports 7 and 8 on the switch are combo ports which support two types of media, copper Ethernet cable (recommended Cat 5e or higher) and fiber using an SFP (mini-GBIC) transceiver. These ports can only support one type of connection at a time. The switch supports most types of SFP transceivers including:

- 1000Mbps LC, multi-mode, SFP Fiber transceiver
- 1000Mbps LC, single mode, 10km, SFP Fiber transceiver
- 1000Mbps LC, single mode, 30km, SFP Fiber transceiver
- 1000Mbps LC, single mode, 50km, SFP Fiber transceiver
- 1000Mbps BiDi LC, single mode, 20km, 1550nm SFP Fiber WDM transceiver
- 1000Mbps BiDi LC, single mode, 20km, 1310nm SFP Fiber WDM transceiver

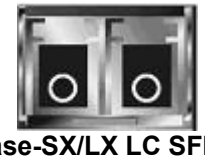

Figure 1-4: 1000Base-SX/LX LC SFP Fiber Transceiver

Figure 1-5: 1000Base-LX BiDi LC SFP Fiber Transceiver

2 Installation

2.1 Installing Switch into 19-Inch Rack

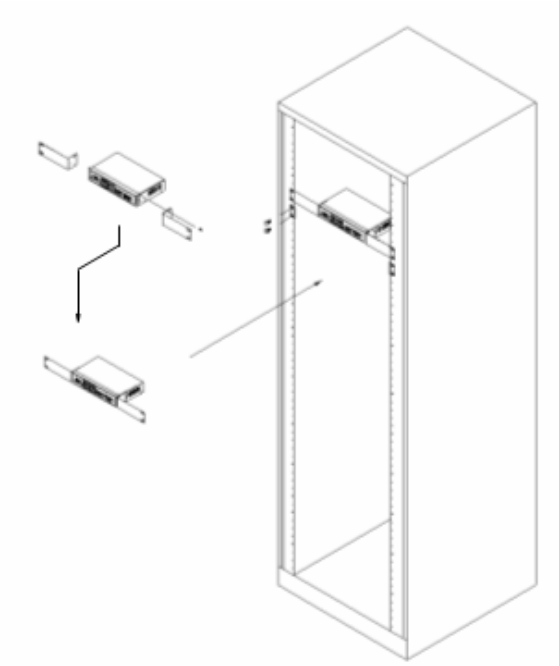

Figure 2-1: Installing the Switch

Caution: Allow proper spacing and air ventilation for the cooling fans on both sides of the switch.

To installing the switch into the rack:

1. Wear a grounding device for electrostatic discharge.
2. Screw the mounting accessory into the sides of the switch (See Figure 2-1).
3. Place the switch into the 19-inch rack in the proper position, then screw the switch to the rack.

2.2 Cable Installation

Before installing the switch, it is recommended that you:

- Wear a grounding device to avoid damage from electrostatic discharge
- Be sure that power switch is set to Off before you plug in the power cord

Copper Cable Installation

The switch supports auto-MDIX meaning that both straight-through and cross-over cables will work regardless of the device on the other end. To ensure that you get full gigabit throughput with the switch, it is recommended that you use category 5e or higher (not category 5) cables.

SFP Transceivers

The SFP slots are hot-swappable, meaning that SFP transceivers can be installed or removed while the switch is on. To install a transceiver:

1. Verify that the SFP module is the right type and form factor for the switch.
2. Slide the module completed into the slot, making sure that the module is properly seated against the connector in the back of the slot
3. Install the fiber cable to connect to the network
4. Repeat the above steps for to install the second transceiver if required

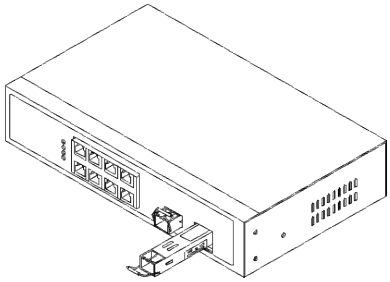

Figure 2-2: Installing SFP Transceivers

Power On

The switch supports 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert the local AC power source to DC power. After the switch is powered on, all LED indicators will light up immediately and then all of them will turn off except for the power LED.

Boot Sequence

After the switch powers on, the bootloader will load the firmware into the memory. This process takes about 30 seconds, after which all of the LEDs will flash once and the switch will then be operational.

2.2.1 Cabling Requirements

Cabling Requirements for Copper Ports

For Fast Ethernet connections, the grade of the cable must be at least Cat 5 with a maximum length of 100 meters.

For Gigabit Ethernet connections, the grade of the cable must be at least Cat 5e with a maximum length of 100 meters.

Cabling Requirements for 1000SX/LX SFP Module

The length of cable supported depends on the types and quality of the transceiver and the cable. Cables are broken up into two categories, multi-mode (MM) and single mode (SM). The latter is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX. For the connector type, they are mainly LC and BIDI LC. Combinations include:

- Gigabit Fiber with multi-mode LC SFP module
- Gigabit Fiber with single-mode LC SFP module
- Gigabit Fiber with BiDi LC 1310nm SFP module
- Gigabit Fiber with BiDi LC 1550nm SFP module

The following table lists the types of fiber supported by the switch:

<table>
<tr><td rowspan="5">IEEE 802.3z Gigabit Ethernet 1000SX 850nm</td><td colspan="4">Multi-mode Fiber Cable and Modal Bandwidth</td></tr>
<tr><td colspan="2">Multi-mode 62.5/125μm</td><td colspan="2">Multi-mode 50/125μm</td></tr>
<tr><td>Modal Bandwidth</td><td>Distance</td><td>Modal Bandwidth</td><td>Distance</td></tr>
<tr><td>160MHz-km</td><td>220m</td><td>400MHz-km</td><td>500m</td></tr>
<tr><td>200MHz-km</td><td>275m</td><td>500MHz-km</td><td>550m</td></tr>
<tr><td rowspan="3">1000Base-LX/LHX/XD/ZX</td><td colspan="4">Single-mode Fiber 9/125μm</td></tr>
<tr><td colspan="4">Single-mode transceiver 1310nm 10km</td></tr>
<tr><td colspan="4">Single-mode transceiver 1550nm 30, 50km</td></tr>
<tr><td rowspan="4">1000Base-LX Single Fiber (BIDI LC)</td><td colspan="2" rowspan="2">Single-Mode 20km</td><td colspan="2">TX(Transmit) 1310 nm</td></tr>
<tr><td colspan="2">RX(Receive) 1550 nm</td></tr>
<tr><td colspan="2" rowspan="2">Single-Mode 20km</td><td colspan="2">TX(Transmit) 1550 nm</td></tr>
<tr><td colspan="2">RX(Receive) 1310 nm</td></tr>
</table>

Table 2-1: Cable Types

Typical Network Topologies

A network with the lowest number of levels of switches will reduce the timing delay between server and client. With this approach, the number of switches in any one path will be minimized, lowering the possibility of a network loop and improving network efficiency. If more than two switches are connected in the same network, select one switch as the Level 1 switch and connect all other switches to it at Level 2. It is recommended to connect the servers to the Level 1 switch. This is a general case if no VLANs or other special requirements are applied.

Case 1: All ports are in the same local area network. Every port can access each other (See Figure 2-3).

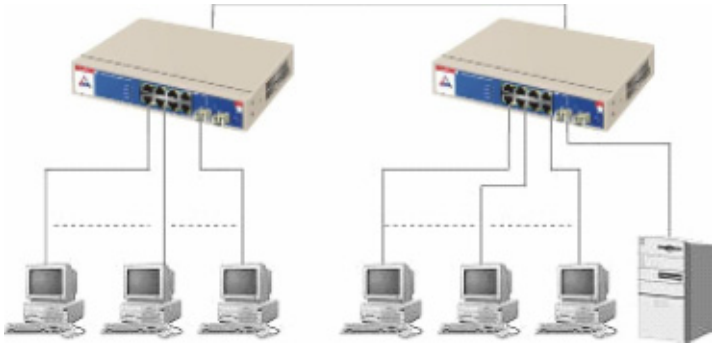

Figure 2-3 No VLAN Configuration Diagram

If VLANs are enabled and configured, each node in the network can only communicate with other nodes in the same VLAN.

Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in terms of physical location. The following diagram shows how each on works and the differences between the two.

Case 2a: Port-based VLAN (See Figure 2-4).

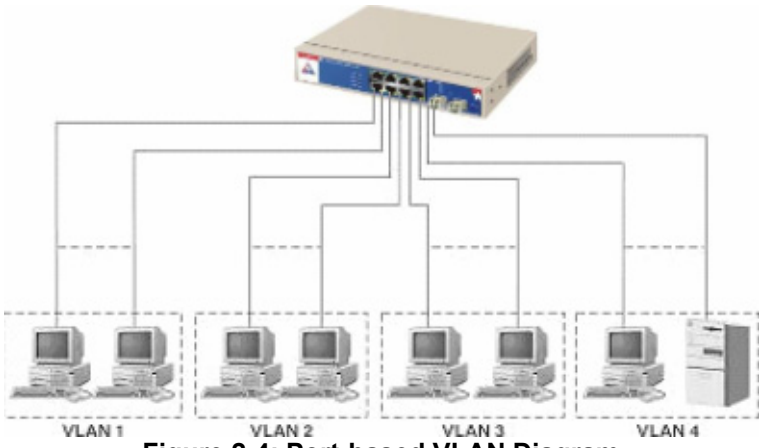

Figure 2-4: Port-based VLAN Diagram

1. The same VLAN members cannot be connected to different switches.
2. Each VLAN member cannot access members of other VLANs.
3. The switch manager has to assign different names for each VLAN group on the switch.

Case 2b: Port-based VLAN (See Figure 2-5).

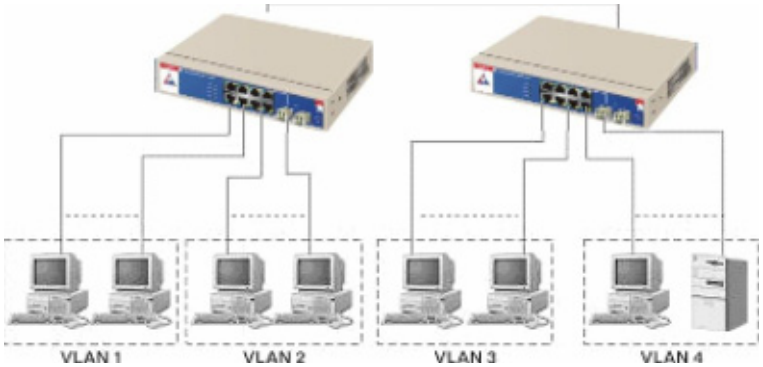

Figure 2-5: Port-based VLAN Diagram on Two Switches

1. VLAN1 members cannot access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members cannot access VLAN1 and VLAN3 members, but they can access VLAN4 members.
3. VLAN3 members cannot access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members cannot access VLAN1 and VLAN3 members, but they can access VLAN2 members.

Case 3: Tag-based VLANs. The same VLAN members can be at different switches with the same VID (See Figure 2-6).

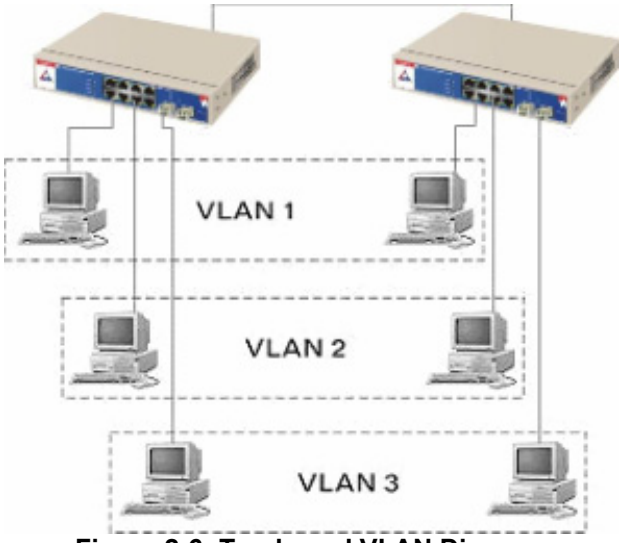

Figure 2-6: Tag-based VLAN Diagram

2.2.2 Configuring the Switch

There are three ways to setup and manage the switch. They are via RS-232 console, command line interface (CLI), and web interface. Users can use any one of them to monitor and configure the switch. To configure the switch using a serial RS-232 connection, refer to Section 4 for connection instructions and the CLI reference.

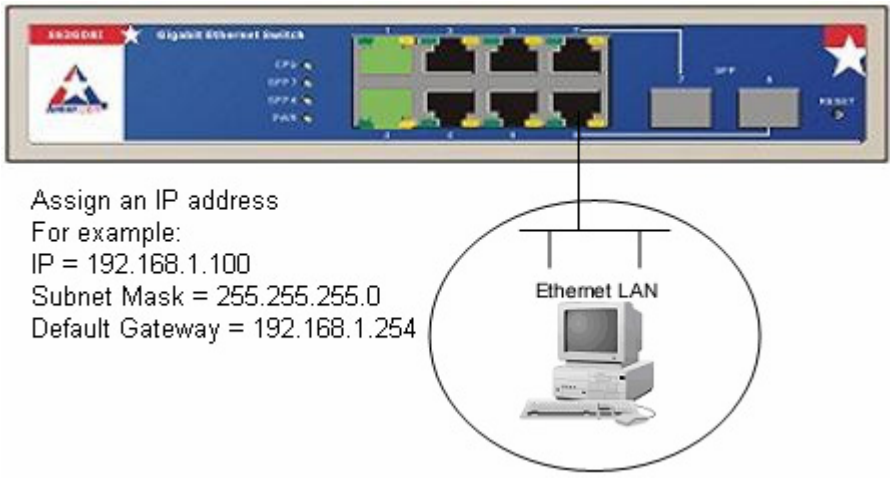

Figure 2-7: Default Settings

To use the switch's web interface to manage the switch, your computer must be connected to the switch via a network cable, and your computer must be in the same subnet as the switch's default settings (Figure 2-7). This can be accomplished by following these steps:

1. Connect an Ethernet cable from your computer to Port 1 on the switch.
2. Ensure that the Link LED for Port 1 lights up, and that a Local Area Connection is shown on your computer.
3. Open the network connections window on your computer (if you are using Windows XP, go to Control Panel -> Network Connections and select Local Area Network, then click Properties).

4. Select Internet Protocol (TCP/IP), then click Properties.
5. Select to use a static IP address or “Use the following IP address”.
6. Enter the following IP address for the computer: “192.168.1.5”
7. Enter the following subnet mask for the computer: “255.255.255.0”
8. Click “OK” and save the settings.
9. Open up a web browser (e.g. Internet Explorer), and enter “http://192.168.1.1” in the address bar.
10. You should now be presented with the login page of the web interface (Figure 2-8). You can log in using the default username “admin” and default password “admin”. See Section 3 for details on using the web interface to manage the switch.

    Note: For best results, it is recommended that you use Microsoft IE 6.0 or above, Netscape V7.1 or above or FireFox V1.00 or above, and have a screen resolution of at least 1024x768.

Figure 2-8: Login Screen

3 Web Interface

Using the web interface, you can monitor and control all aspects of the switch, including port status and activity, spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, illegal access records.

The default settings of the switch are as follows:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	Admin

Table 3-1: Default Settings

To connect and log into the switch, refer to section 2.2.2. After logging into the switch using the default username and password, you will see the main menu.

> **Note:** The switch only allows one user to log in and manage the switch at a time. Any other users who log in after the first user is already in, regardless of their access level, will only be able to monitor the status of the switch. Up to three users can be logged into the switch simultaneously.

Password Recovery

If you forget the password to log into the switch, click the link “Forget Password?” in GUI or type “Ctrl+Z” in the CLI login screen. The switch will display a serial number used to recover the password (See Figure 3-1). Write down the serial number and email it to Amer.com in order to get a temporary password. Use this new password as the Username and Password, and it will allow you to login to the switch temporarily. This temporary password will only work once, therefore you should change your password immediately after you successfully login to the switch.

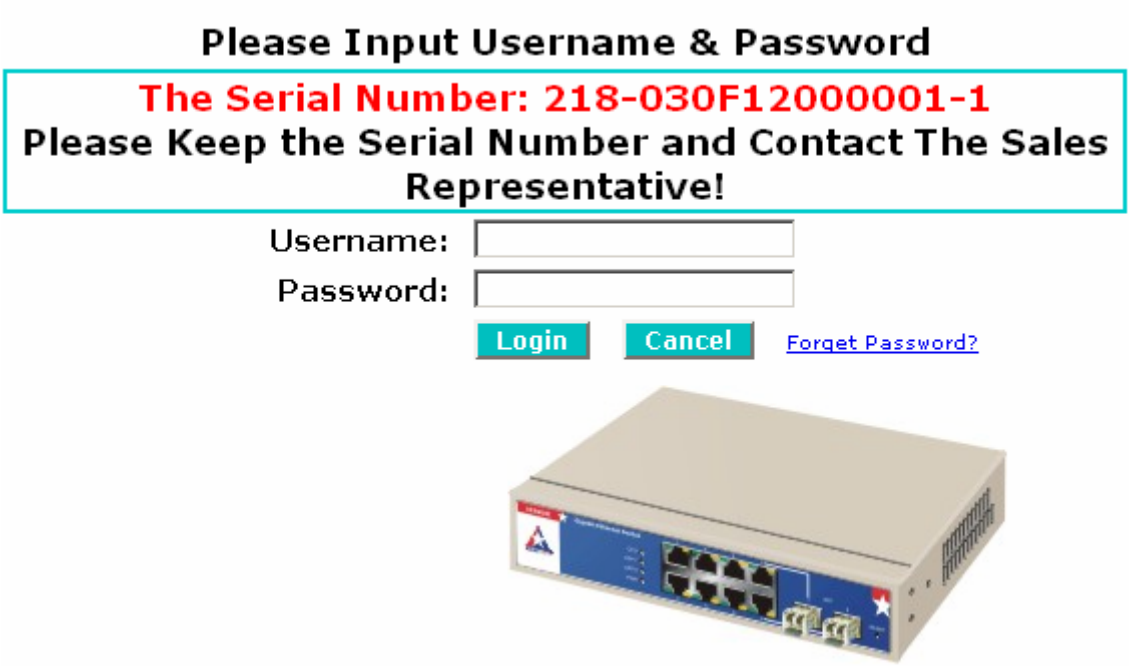

Figure 3-1: Password Recovery Screen

3.1 Home Page

After you login, the switch will display the System Information page (figure 3-2). This page shows you some basic information about the switch, including “Model Name”, “System Description”, “Location”, “Contact”, “Device Name”, “System Up Time”, “Current Time”, “BIOS Version”, “Firmware Version”, “Hardware-Mechanical Version”, “Serial Number”, “Host IP Address”, “Host Mac Address”, “Device Port”, “RAM Size” and “Flash Size”.

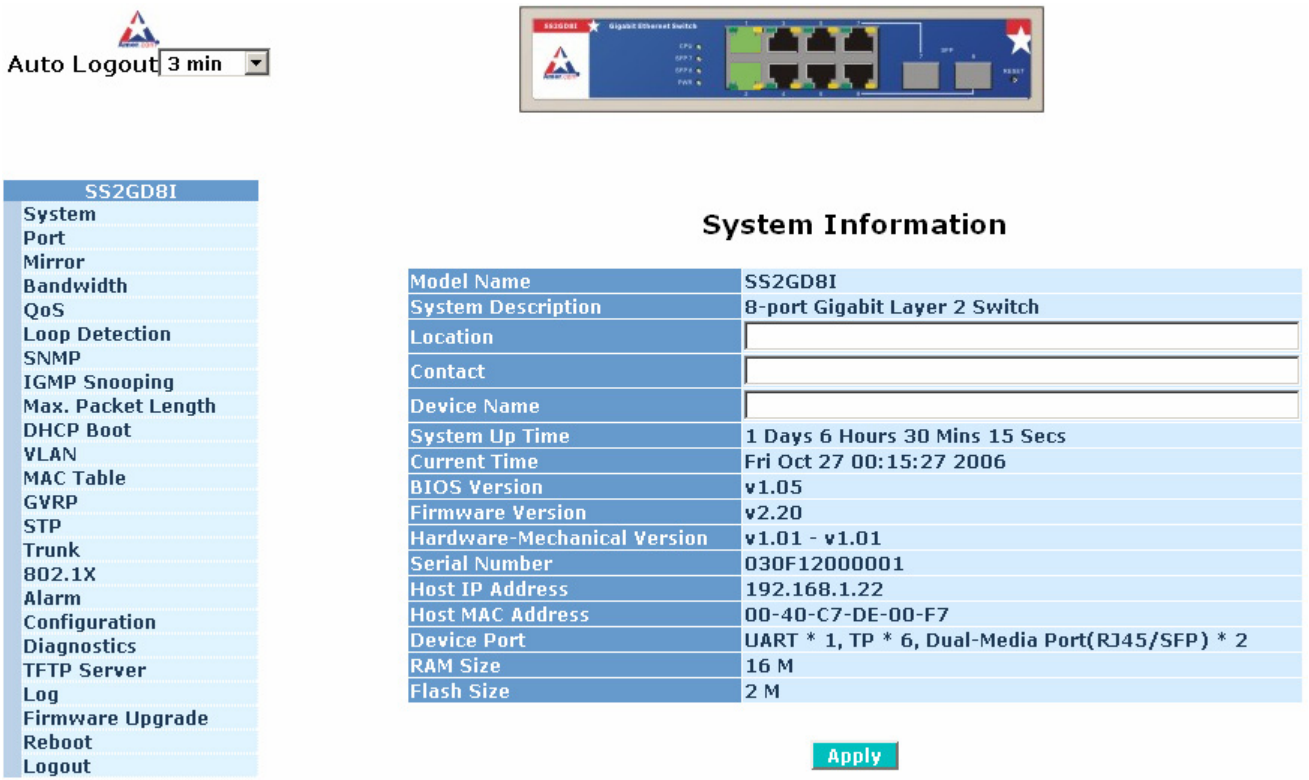

Figure 3-2: System Information Page

The picture of the switch at the top will display all ports which currently have an active link in green. For the SFP modules, a transceiver will be shown in the picture if one is installed in the slot. The transceiver will also light up green if there is an active connection on that link.

You can also click on any of the ports in the picture to open a new window that displays information specific to that port (figure 3-3). On this page, you can view all of the information for traffic on this port with a quick glance.

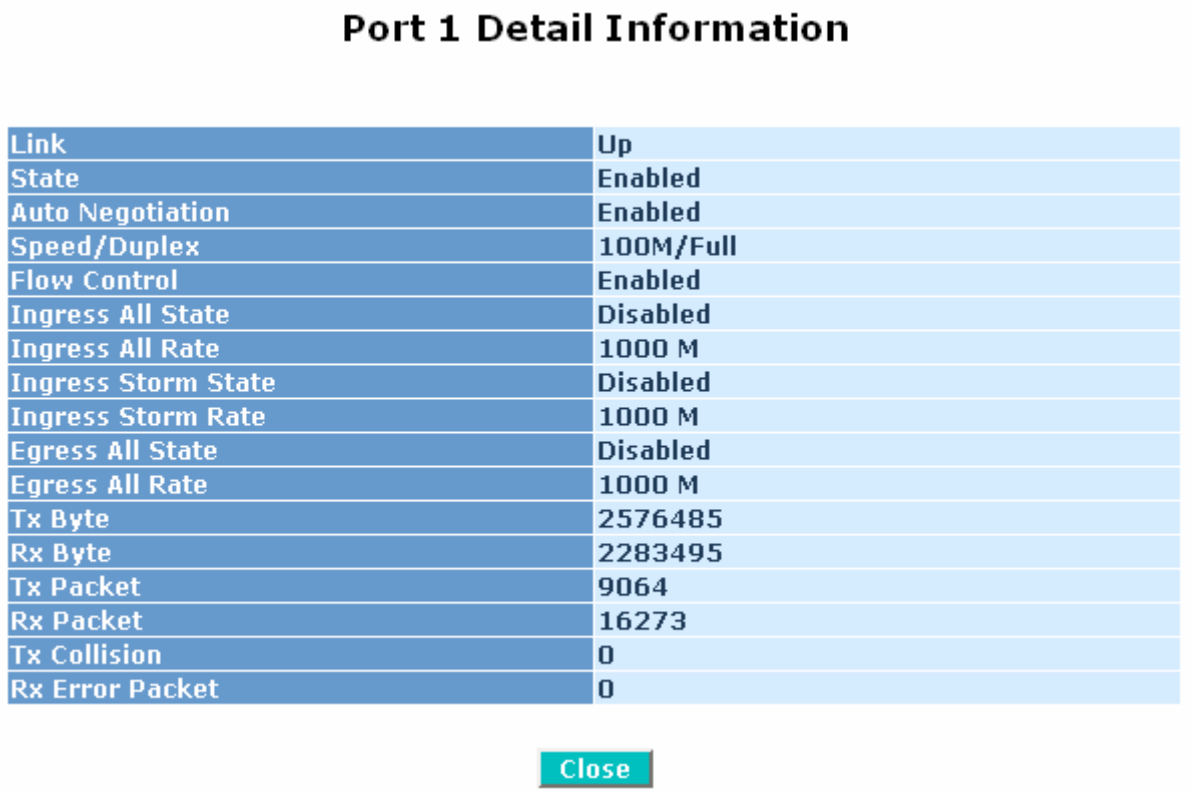

Figure 3-3: Port Information Page

On the left-top corner of the home page, there is a dropdown list to set the Auto Logout time. For security purposes, you will automatically be logged out after a period of inactivity. You can change the amount of time the switch waits before automatically logging you out by selecting a duration from this dropdown list. You can also disable the auto-logout feature by selecting “Off” from the list. Once you are logged out, you will need to log back in through the login page.

The menu on the left-hand side of the screen will allow you to navigate through the web interface and manage all of the different features of the switch. Clicking on one of the menu options will reveal a list of submenu items that can be selected. Each menu item will be described in detail in the following sections.

3.1.1 System Information

The System Information page under the System menu (Figure 3-2) shows the basic system information for the switch. The fields on this page are described below:

Model name: The model name of the switch.

System description: A description of the switch including the number of ports and management level.

Location: A description of the physical location of the switch as defined by the user.

Contact: The contact information for the network administrator in the event of a problem with the switch as defined by the user.

Device name: The name of the switch as defined by the user, the default is “SS2GD8I”.

System up time: The amount of time that the switch has been operational. This number is reset if the switch is powered off.

Current time: The system time of the switch.

BIOS version: The version of the BIOS in the switch.

Firmware version: The firmware version on the switch.

Hardware-Mechanical version: The hardware and mechanical version of the switch. The number before the hyphen is the hardware version; the one after the hyphen is the mechanical version.

Serial number: The serial number as assigned by the manufacturer.

Host IP address: The IP address of the switch.

Host MAC address: The Ethernet MAC address the switch.

Device Port: The types and numbers of ports in the switch.

RAM size: The size of the DRAM in this switch.

Flash size: The size of the flash memory in this switch.

3.1.2 IP Configuration

The IP Configuration page under the System menu (Figure 3-4) allows you to set the IP address of the switch. The switch supports both static and dynamic IP addresses. When you change the IP address of the switch, you must reboot the switch in order for the change to take effect. You will also have to use the new IP address to access the web interface and CLI for the switch.

> **Note:** If you select dynamic IP address, the switch will automatically get an IP address from your DHCP server on the network. In order to determine the IP address received by the switch, you will either need to log in through the console port, or view the DHCP table on your DHCP server.

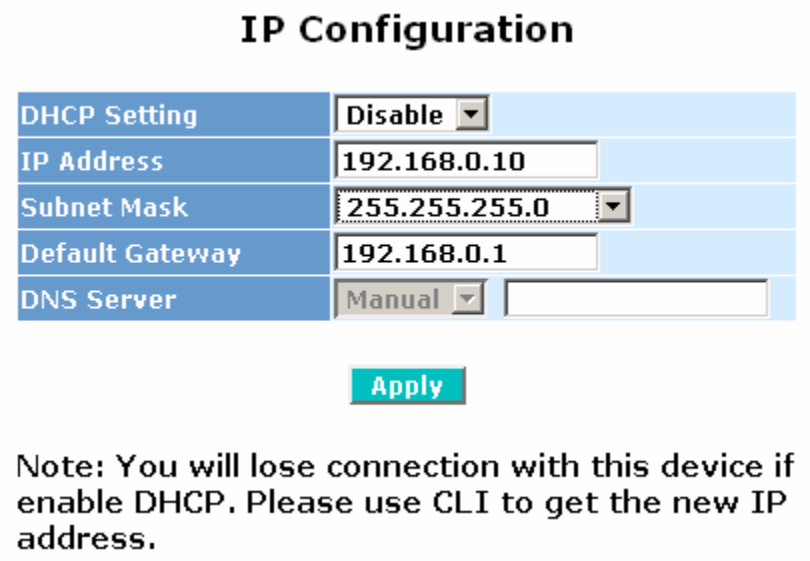

Figure 3-4: IP Configuration Page

DHCP Setting: If set to “Enable”, the switch will retrieve its IP address from a DHCP server on the network, thereby getting a dynamic IP address. If the DHCP server is down or does not exist, the switch will show that the IP address is being requested until the DHCP server is up. Until it gets an IP address, the switch will not continue booting. If set to “Disable”, you will have to manually input the IP address in the fields below.

IP address: Allows you to manually set the switch’s IP address if DHCP Setting is set to “Disable”, otherwise this field is not used. Default: 192.168.1.1

Subnet mask: Allows you to manually set the switch’s subnet mask if DHCP Setting is set to “Disable”, otherwise this field is not used. Default: 255.255.255.0

Default gateway: Allows you to manually set the IP address for your network gateway, which is typically a router or bridge to the internet or other subnet. All packets which are addressed to a device that is not in the switch's routing table will be sent to the default gateway. Default: 192.168.1.254

DNS: The Domain Name Server used to serve the translation between IP addresses and domain names. If set to "Manual", it must be entered manually by the user. If set to "Dynamic", it will take the DNS server given by the DHCP server. DHCP Setting must be set to "Enable" for this to work. Default: 0.0.0.0

3.1.3 Time

The Time page under the System menu (Figure 3-5) allows you to set the system time for the switch. The time can either be set manually or by using an NTP (network time protocol) server which are freely available on the internet.

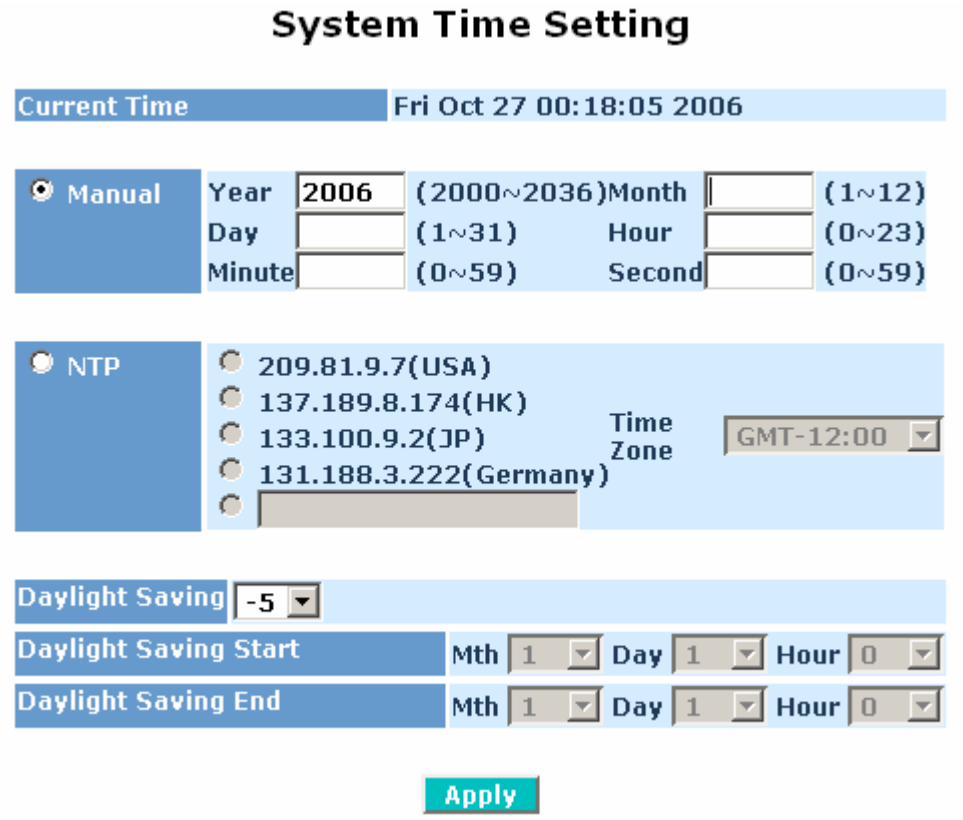

Figure 3-5: System Time Page

NTP is a standard protocol used to synchronize system clocks over a network or the internet. The switch includes four common NTP server IP addresses which you can choose from, or you can enter your own. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

Current Time: Shows the current time of the switch.

Manual: Allows you to manually set the time on the switch. Enter the desired parameters and click "Apply" to set the time. There is no time zone setting in Manual mode.

NTP: Allows you to select an NTP server for the switch to use to obtain its system time. You will also need to select your time zone to get the correct time from the server. The switch will synchronize the time shortly after pressing "Apply". The switch supports time zones from -12 to +13 in 1 hour increments.

Daylight Saving: Allows you to set the daylight saving time settings for your region. If this is set, the time will be changed by a certain amount on the start date, and will be change back on the end date. Typically, the amount of change would be +1 (turn the clock ahead), and it will start in the Spring and end in the

Fall. Available choices for the time change are from -5 to +5 in one hour increments. Setting this to zero will disable daylight saving time. If the value is non-zero, you have to set the starting/ending date as well; otherwise the daylight saving function will not be activated.

3.1.4 Account Configuration

The Account Configuration page under the System menu (Figure 3-6) allows you to manage the users who can manage the switch. Only administrators can create, modify or delete user accounts. Only one Administrator is allowed and cannot be deleted, and up to four Guest accounts are allowed. The administrator has full access rights to the switch, while Guests only have read-only access. Administrators are also able to modify passwords for all accounts, while guests are only able to modify the password for their own account on this page. The default settings for the Administrator account is “admin” for both username and password, and for the guest is “guest” for both username and password.

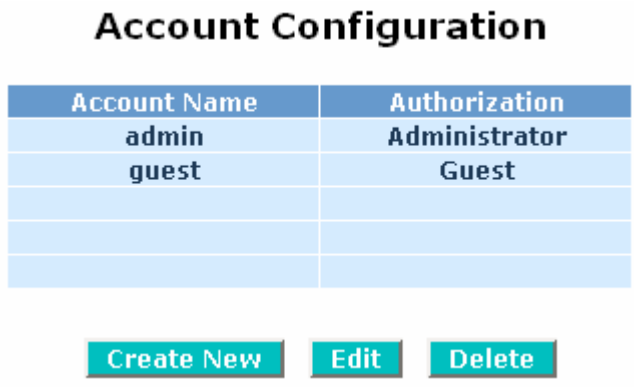

Figure 3-6: Account Configuration Page

3.1.5 Management Policy

The Management Policy page under the System menu (Figure 3-7) allows you to set rules for users to access the management interface of the switch, be it web, telnet, or SNMP. You can accept or deny access based on VID, IP address, physical port connection, and access type. There are several scenarios for defining rules:

No rules are defined: The switch will accept all incoming connections.

Only Accept rules are defined: The switch will only accept connections defined by the Accept rules, and will Deny all other connection attempts.

Only Deny rules are defined: The switch will accept any connections that do not defined the Deny rules.

Both Accept and Deny rules are defined: The switch will only accept connections defined by the Accept rules and are not defined by the Deny rules, and Deny all other attempts as well.

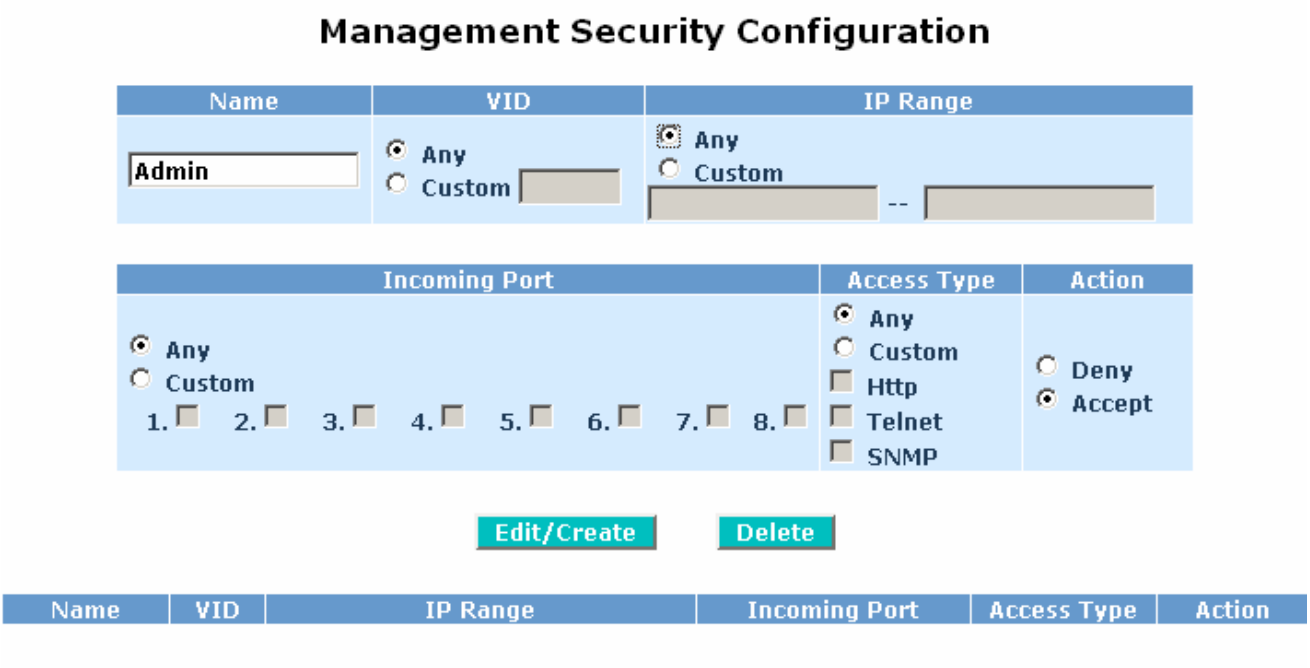

Figure 3-7: Management Policy Page

Name: A name for the rule made up of letters and numbers up to 8 characters.

VID: If set to "Any", the rule applies to users from any VLAN, otherwise you can enter a specific VID to limit the rule. Valid VID range is from 1 to 4094.

IP Range: If set to "Any", the rule applies to users with any IP address, otherwise you can enter a range of IP addresses to restrict which users the rule will apply to. The valid IP range is from 0.0.0.0 to 255.255.255.255.

Incoming Port: If set to "Any", the rule applies to users connected to any physical port, otherwise you can select which physical ports apply to the rule. The numbers here correspond to the numbers on the physical ports on the switch.

Access Type: If set to "Any", the rule applies to users using any management interface, otherwise you can select which management interfaces apply to the rule. Valid options are HTTP, Telnet, and SNMP.

Action: Allows you to select whether to Allow access to users covered by this rule, or the Deny access to them.

Edit/Create: After entering the parameters above, click this button to save the new rule, or the modify an existing one.

Delete: Remove an existing entry from the table.

3.1.6 Virtual Stack

The Virtual Stack page under the System menu (Figure 3-8) allows you set virtual stack settings for the switch. Multiple switches in the same LAN can be grouped together in order to simplify management through the web interface. All switches in the same stack can be managed using the IP address of the Master switch.

If Virtual Stack is configured, two rows of buttons (16 in total) will appear at the top of the web interface after logging into the master switch to allow for selecting the device to manage. By using these buttons, you can select which switch in the group to connect to and manage without logging into each switch individually.

The button on the far left of the top row represents the master switch. The background color of the active switch will be highlight in green.

Note: If you log into a switch using the console, it will disable the virtual stack temporarily.

The name of the device is shown as the station address (the last number of the IP address) plus the name of the switch, concatenated with an underscore (e.g. 100_SS2GD8I) for a switch with an IP address 192.168.0.100 and name “SS2GD8I”. Otherwise it will show ” ---- “ if there is no switch active there.

Once the devices have successfully joined the group, then they will only be manageable through the Master device, and will be unable to be managed via telnet/console/web individually.

Up to 16 devices can be grouped in a Virtual Stack, however only one Master is allowed to exist in each group at a time. For redundancy, you may configure more than two devices as Master devices. However, the Master device with the smallest MAC value will be set as the Master. All of these 16 devices can become the Master device and back up each other.

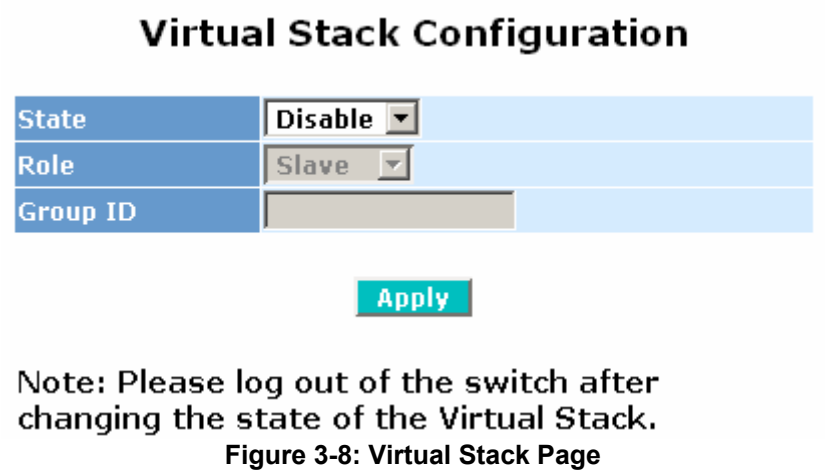

Figure 3-8: Virtual Stack Page

State: Used to enable or disable virtual stacking.

Role: The role that the switch should play in the virtual stack, either Slave or Master.

Group ID: The group identifier (GID) for the VSM. All switches in the same group must have the same Group ID. Valid values are letters, numbers, and underscores up to 15 characters in length.

3.2 Port Configuration

Four functions, including Port Status, Port Configuration, Simple Counter and Detail Counter are contained in the Port menu for port monitoring and management. Each of them will be described in detail in the following sections.

3.2.1 Port Status

The Port Status page (Figure 3-9) displays information for all of the ports on the switch including link status, port state, auto-negotiation status, speed/duplex and flow control. The page will automatically refresh every 5 seconds. Clicking on a port will open a status window as shown in Figure 3-3.

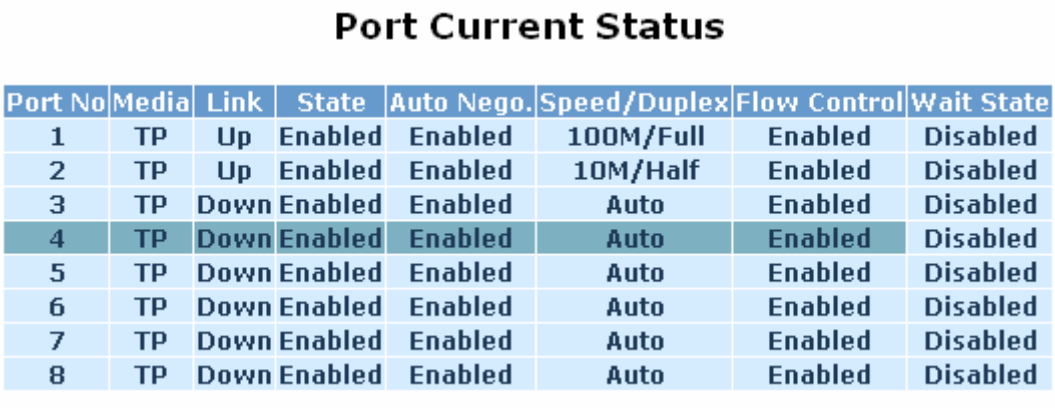
Port Current Status
Port No Media Link State Auto Nego. Speed/Duplex Flow Control Wait State
1 TP Up Enabled Enabled 100M/Full Enabled Disabled
2 TP Up Enabled Enabled 10M/Half Enabled Disabled
3 TP Down Enabled Enabled Auto Enabled Disabled
4 TP Down Enabled Enabled Auto Enabled Disabled
5 TP Down Enabled Enabled Auto Enabled Disabled
6 TP Down Enabled Enabled Auto Enabled Disabled
7 TP Down Enabled Enabled Auto Enabled Disabled
8 TP Down Enabled Enabled Auto Enabled Disabled

Figure 3-9: Port Status Page

Port No: The port number, ranging from 1-8. Both ports 7 and 8 are optional modules.

Media: Shows the media type of the port. Ports 1-6 are twisted pair (TP) or copper, while ports 7 and 8 could be twisted pair or fiber.

Link: Shows if the link is active or not. If the link is connected to a working device, the Link will be “Up”; otherwise, it will be “Down”.

State: Shows whether the port is “Enabled” or “Disabled”. When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transmitted through this port. Port State is configured by the user.

Auto Negotiation: Shows whether the port has speed and duplex auto-negotiation enabled on or not. When “Enabled”, the switch will automatically negotiation the best speed and duplex supported by both devices. If “Disabled”, it must be set manually by the user. This option is set by the user.

Speed / Duplex Mode: Displays the speed and duplex of the port. There are three speeds 10Mbps, 100Mbps and 1000Mbps supported for TP media, and the duplex supported is half duplex and full duplex. If the media is 1Gbps fiber, it can be 1000Mbps only.

Flow Control: Shows the port’s flow control status.

Wait State: For 10/100M ports, this value is irrelevant. For Gigabit ports, setting of Wait State will remove the issue with ignored pause frames but result in the minimum interframe gap being at least 14 bytes instead of the usual 12 bytes. This applies to non-congested traffic as well. The larger interframe gap will result in throughput rates less than 100%. For example, for a stream of 64-byte frames and a stream of 1518-byte frames, their maximum throughput is 97.7% and 99.9% respectively.

3.2.2 Port Configuration

The Port Configuration page (Figure 3-10) is used to change the settings of each of the ports.

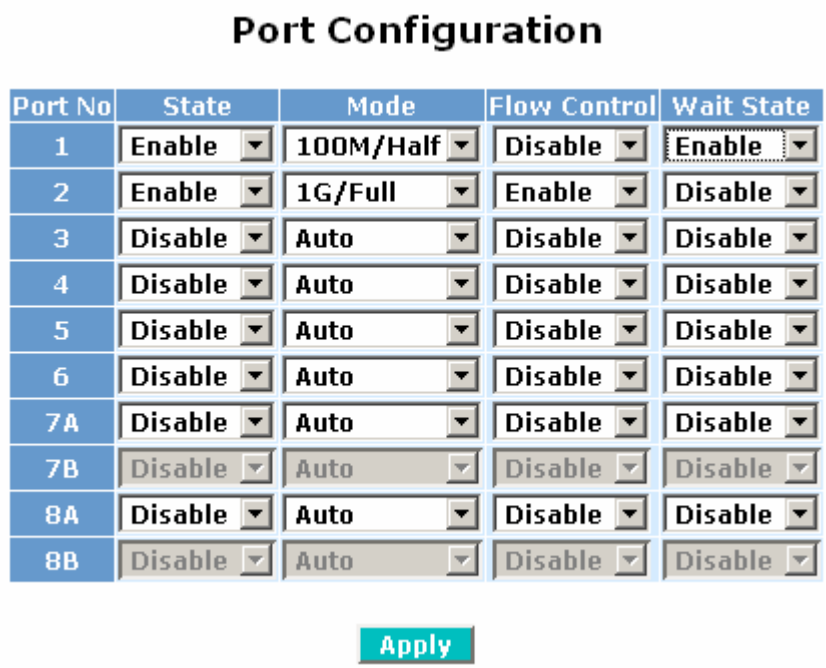

Figure 3-10: Port Configuration Page

State: Either “Enable” or “Disable” the port, allowing traffic to pass through it or not. Default: Enable.

Mode: Sets the speed and duplex of the port. If the connection is 1Gbps, the speed is always 1000Mbps and the duplex is full only. If the media is 10/100Mbps copper, the Speed/Duplex is comprised of a combination of speed (10 or 100Mbps) and duplex mode (full duplex or half duplex). Mode can also be set to auto-negotiation (Auto) mode.

Flow Control: Either set to “Enable” or “Disable”. If flow control is set Enable, both parties can send PAUSE frames to the transmitting device(s) if the receiving port is too busy to handle it. When it is set Disable, there will be no flow control in the port. It drops the packet if there is too much traffic to handle. Default: Enable.

Wait State: For more details about this parameter please refer to section 3.2.1. Default: Disable.

3.2.3 Simple Counter

The Simple Counter page (Figure 3-11) displays the basic traffic information for the switch. The user can select how often the page refreshes itself, and can also click “Reset” to reset all of the counters. Each counter can count up to 20 digits long before automatically resetting to 0.

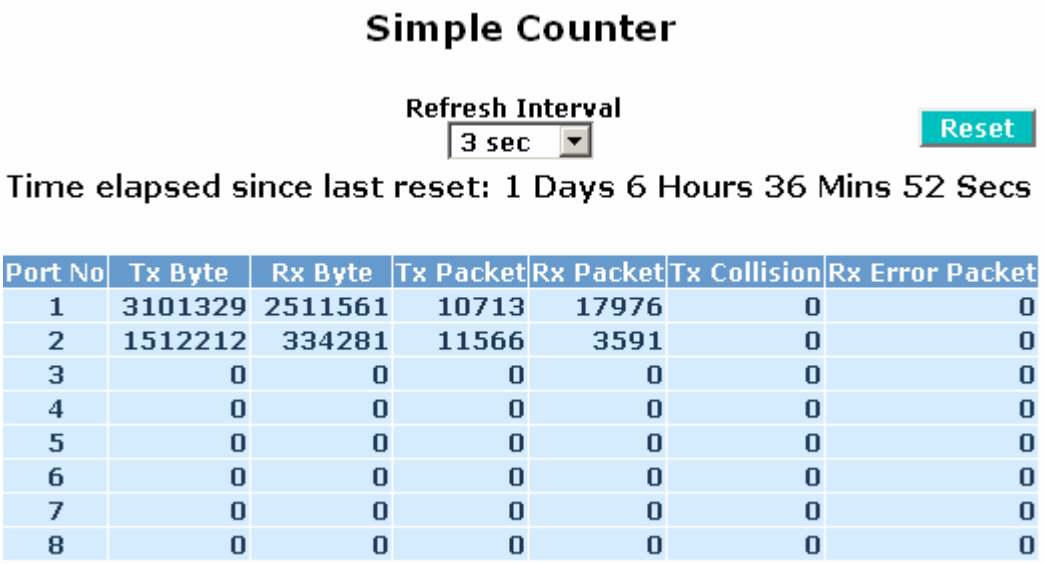
Simple Counter
Refresh Interval
3 sec
Reset
Time elapsed since last reset: 1 Days 6 Hours 36 Mins 52 Secs
Port No Tx Byte Rx Byte Tx Packet Rx Packet Tx Collision Rx Error Packet
1 3101329 2511561 10713 17976 0 0
2 1512212 334281 11566 3591 0 0
3 0 0 0 0 0 0
4 0 0 0 0 0 0
5 0 0 0 0 0 0
6 0 0 0 0 0 0
7 0 0 0 0 0 0
8 0 0 0 0 0 0

Figure 3-11: Simple Counter Page

Tx Byte: Total transmitted bytes.

Rx Byte: Total received bytes.

Tx Packet: Total number of packets transmitted.

Rx Packet: Total number of packets received.

Tx Collision: Number of collisions experienced while transmitting.

Rx Error Packet: Number of bad packets received.

3.2.4 Detail Counter

The Detail Counter Page (Figure 3-12) displays the detailed traffic information for the switch. The user can select which port to view the details for, and how often the page refreshes itself, and can also click “Reset” to reset all of the counters. Each counter can count up to 20 digits long before automatically resetting to 0.

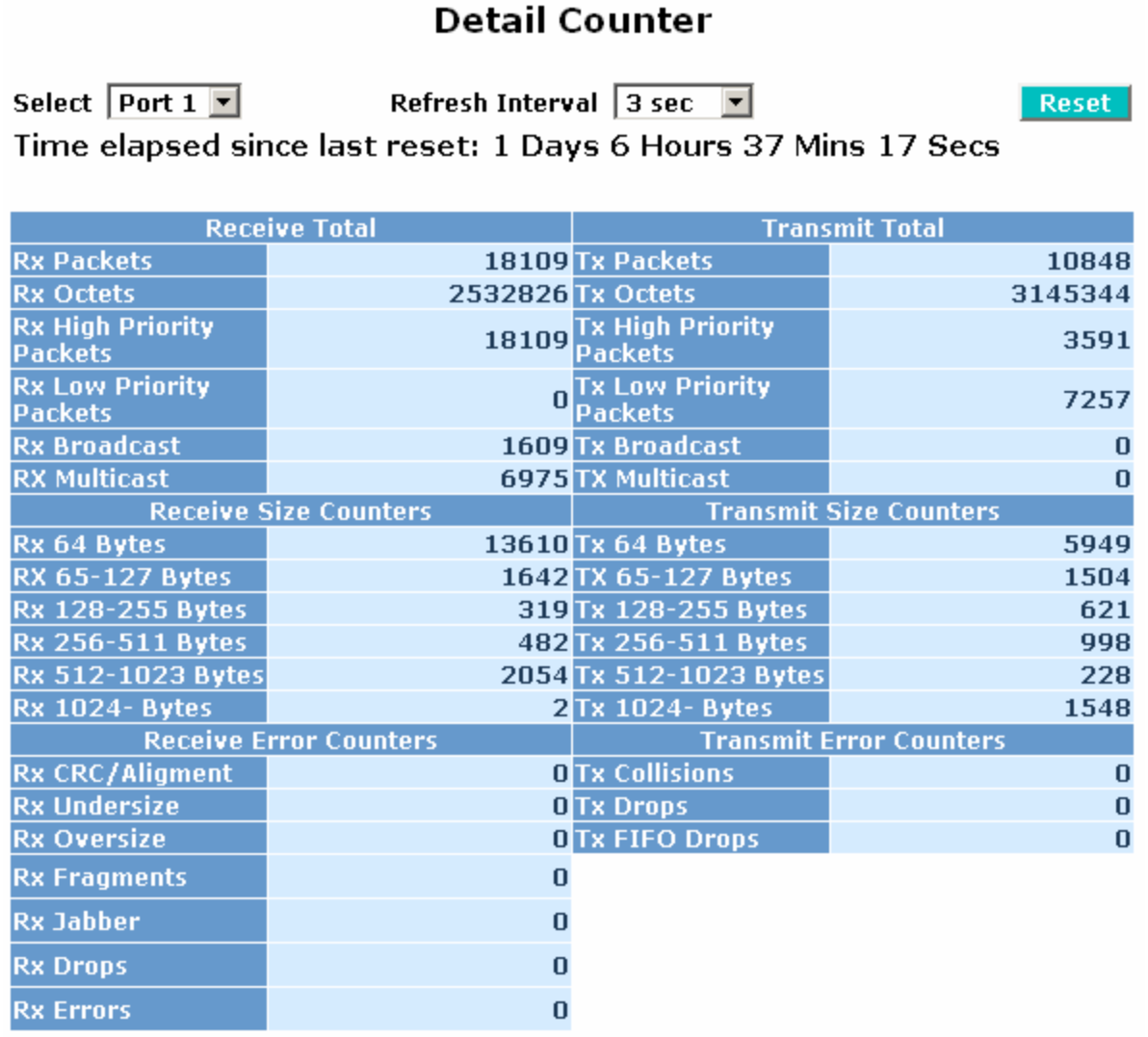

Figure 3-12: Detail Counter Page

Rx Packets: The number of the packet received.

RX Octets: Total received bytes.

Rx High Priority Packets: Number of received packets classified as high priority.

Rx Low Priority Packets: Number of received packets classified as low priority.

Rx Broadcast: The number of the received broadcast packets.

Rx Multicast: The number of the received multicast packets.

Tx Packets: The number of the packet transmitted.

TX Octets: Total transmitted bytes.

Tx High Priority Packets: Number of transmitted packets classified as high priority.

Tx Low Priority Packets: Number of transmitted packets classified as low priority.

Tx Broadcast: The number of the transmitted broadcast packets.

Tx Multicast: The number of the transmitted multicast packets.

Rx 64 Bytes: Number of 64-byte frames in both good and bad packets received.

Rx 65-127 Bytes: Number of 65 - 126-byte frames in both good and bad packets received.

Rx 128-255 Bytes: Number of 127 - 255-byte frames in both good and bad packets received.

Rx 256-511 Bytes: Number of 256 - 511-byte frames in both good and bad packets received.

Rx 512-1023 Bytes: Number of 512 - 1023-byte frames in both good and bad packets received.

Rx 1024-Bytes: Number of 1024 - max_length-byte frames in both good and bad packets received.

Tx 64 Bytes: Number of 64-byte frames in both good and bad packets transmitted.

Tx 65-127 Bytes: Number of 65 - 126-byte frames in both good and bad packets transmitted.

Tx 128-255 Bytes: Number of 127 - 255-byte frames in both good and bad packets transmitted.

Tx 256-511 Bytes: Number of 256 - 511-byte frames in both good and bad packets transmitted.

Tx 512-1023 Bytes: Number of 512 - 1023-byte frames in both good and bad packets transmitted.

Tx 1024-Bytes: Number of 1024 - max_length-byte frames in both good and bad packets transmitted.

Rx CRC/Alignment: Number of Alignment errors and CRC error packets received.

Rx Undersize: Number of short frames (<64 Bytes) with valid CRC received.

Rx Oversize: Number of long frames (according to max_length register) with valid CRC received.

Rx Fragments: Number of short frames (< 64 bytes) with invalid CRC received.

Rx Jabber: Number of long frames (according tomax_length register) with invalid CRC received.

Rx Drops: Frames dropped due to lack of receiving buffer space.

Rx Errors: Number of the error packets received.

Tx Collisions: Number of collisions experienced while transmitting frames.

Tx Drops: Number of frames dropped due to excessive collision, late collision, or frame aging.

Tx FIFO Drops: Number of frames dropped due to the lack of transmitting buffer space.

3.3 Mirror

The Mirror page (Figure 3-13) allows you to configure port mirroring on the switch. Port mirroring allows you to duplicate all of the traffic going to one or more ports on to your monitoring port. This is typically used for diagnosing and troubleshooting problems on the network. For example, if port 1 is the monitoring port, and ports 2 and 3 are monitored ports, then all traffic going to ports 2 and 3 will be copied to port 1.

> **Note:** When using port mirroring, you should avoid setting a port to be a monitoring port and an aggregated port at the same time to avoid conflicts.

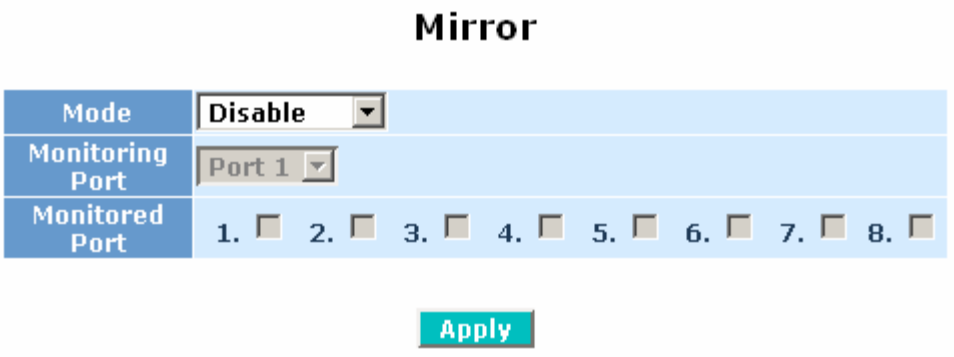

Figure 3-13: Port Mirroring Page

Mode: Used to "Enable" or "Disable" port mirroring. Default is Disable.

Monitoring Port: Set the port that will be monitoring the other ports. Default is Port 1.

Monitored Port: Set the port(s) to be monitored. Place an X beside the number of the port(s) to monitor. The Monitoring port should not be selected as a Monitored port.

3.4 Bandwidth Management

The Bandwidth Management page (Figure 3-14) allows you to set both incoming and outgoing bandwidth limitations for each port.

> **Note:** Each port on the switch has its own 16KB packet buffer. The packet buffer size will be reduced when the bandwidth rate limitation is enabled, which may cause jumbo frames not to be forwarded. Jumbo frames should not be used in conjunction with bandwidth limitations.

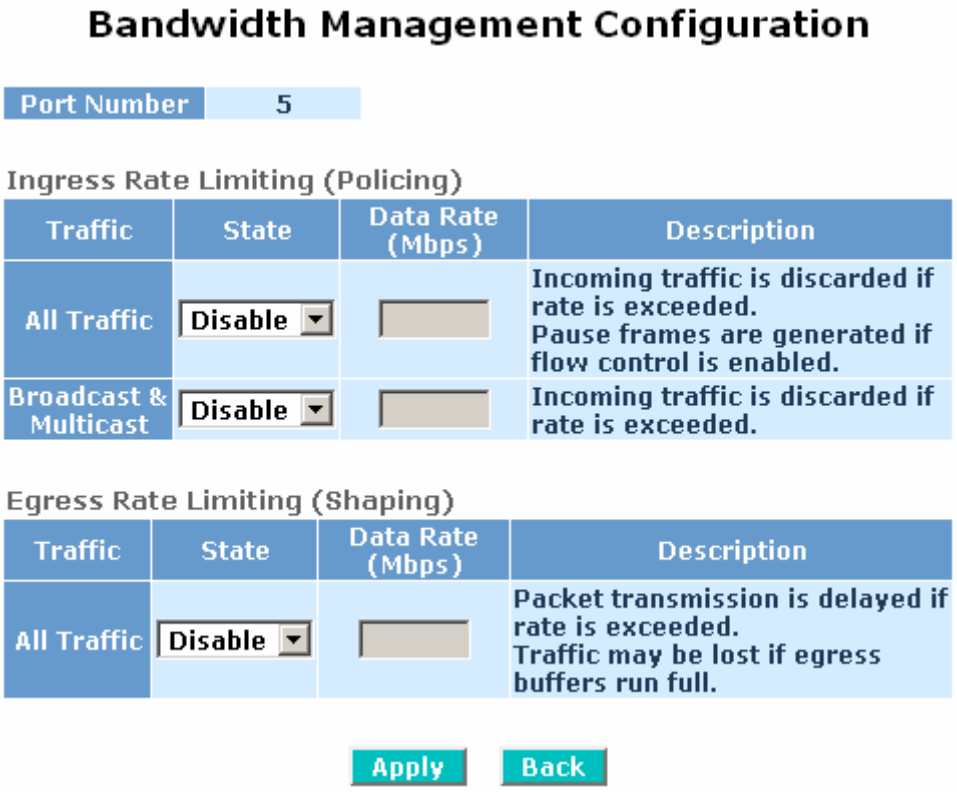

Figure 3-14: Bandwidth Management Page

Port Number: The port that is currently being configured. Can be set to ports 1 through 8.

All Traffic for Ingress Rate Limiting(Policing): Sets the limit of Ingress (incoming) bandwidth for all traffic. Incoming traffic will be discarded if the rate exceeds the value set under Data Rate. Pause frames are also generated if flow control is enabled. Valid range is from 0 to 1000.

Broadcast & Multicasat for Ingress Rate Limiting (Policing): Sets the limit of Ingress (incoming) bandwidth for broadcast and multicast traffic only. Incoming broadcast and multicast traffic will be discarded if the rate exceeds the value set under Data Rate. Valid range is from 0 to 1000.

All Traffic for Egress Rate Limiting (Shaping): Sets the limit of Egress (outgoing) bandwidth for the all traffic. Packet transmission will be delayed if the rate exceeds the value set under Data Rate. Traffic may be lost if egress buffers become full. Valid range is from 0 to 1000.

3.5 QoS (Quality of Service) Configuration

The QoS Configuration page (Figure 3-15) allows you to configure the QoS (Quality of Service) settings for the switch. The switch supports 5 kinds of QoS functions. There is Per Port Priority that allows you to assign a priority to each port, VLAN Tag priority that prioritizes packets based on their VLAN tag, IP TOS Classification, IP TCP/UDP Port Classification and IP DiffServ Classification.

The Default Class determines the QoS class to assign to packets that are not covered by the QoS type selected. For example, if you use VLAN Tag Priority mode, and then choose Default Class as High, then the priority of packets with no tag will be considered as High priority. The initial value of the Default Class is High.

The switch supports two priority classes, High and Low. For example, if Ports 2 and 3 both transmit packets at 1Gbps to Port 1, and Port 2 is set to high priority and Port 3 is low priority, then the packets from Port 3 will be dropped when congestion occurs because Port 2 has a higher priority.

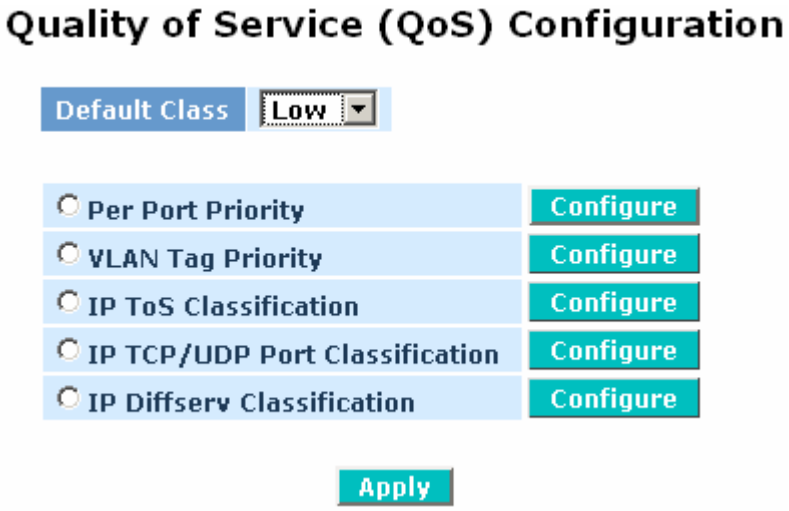

Figure 3-15: QoS Configuration Page

Per Port Priority

For Per Port Priority (Figure 3-16), you can select which priority to assign each of the 8 ports on the switch.

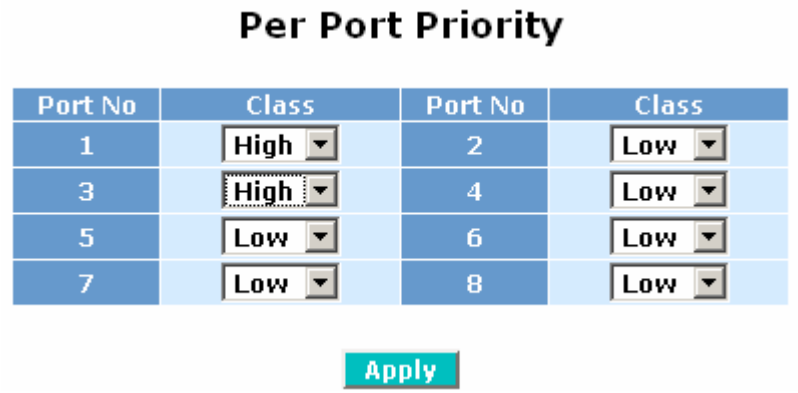

Figure 3-16: Per Port Priority

VLAN TAG Priority

For VLAN Tag Priority (Figure 3-17), you can set the mapping of VLAN tags to the two priority levels in the switch. VLAN Tags support up to 8 values using a combination of three binary numbers. That is, 000 represent 0, 001 represents 1, 010 represents 2, and so forth. Each of these levels can be mapped to either High or Low priority to be used by the switch. You can either set the mapping for all of the ports at the same time, or do it per port by selecting the port to configure on the left. Click “Apply” to save the changes.

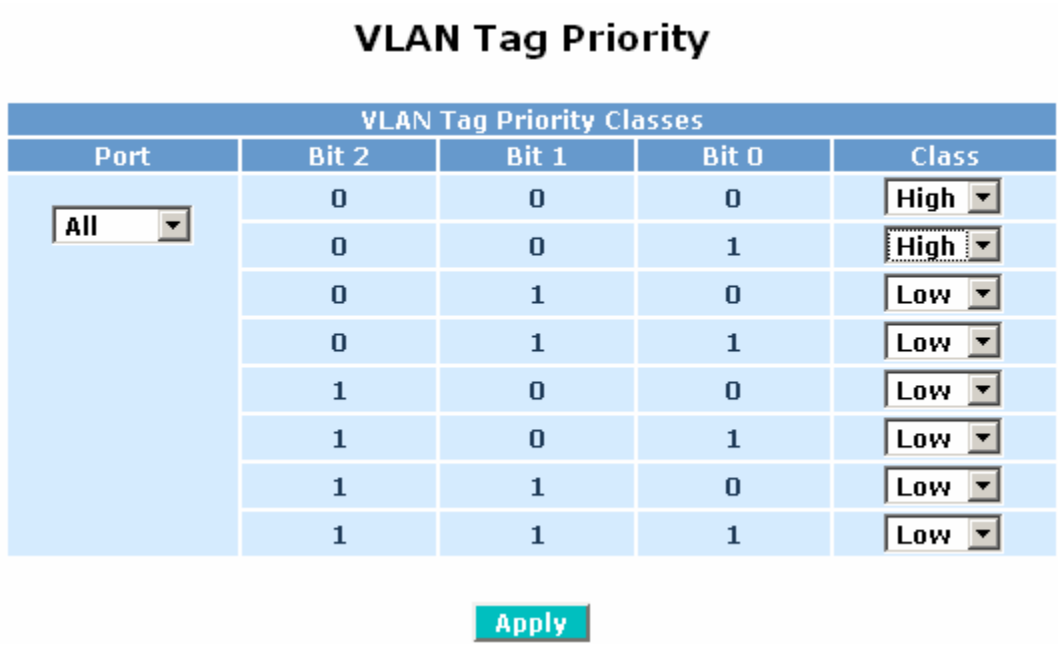

Figure 3-17: VLAN Tag Priority

Quality of Service ToS Configiruation

Quality of Service ToS Configuration (Figure 3-18) works similarly to VLAN Tag Priority, except that the ToS field (bits 5-7) of the packet is used instead of the QOS field in the VLAN tag. The mapping works in the same way, mapping high or low priority to the value of the ToS field.

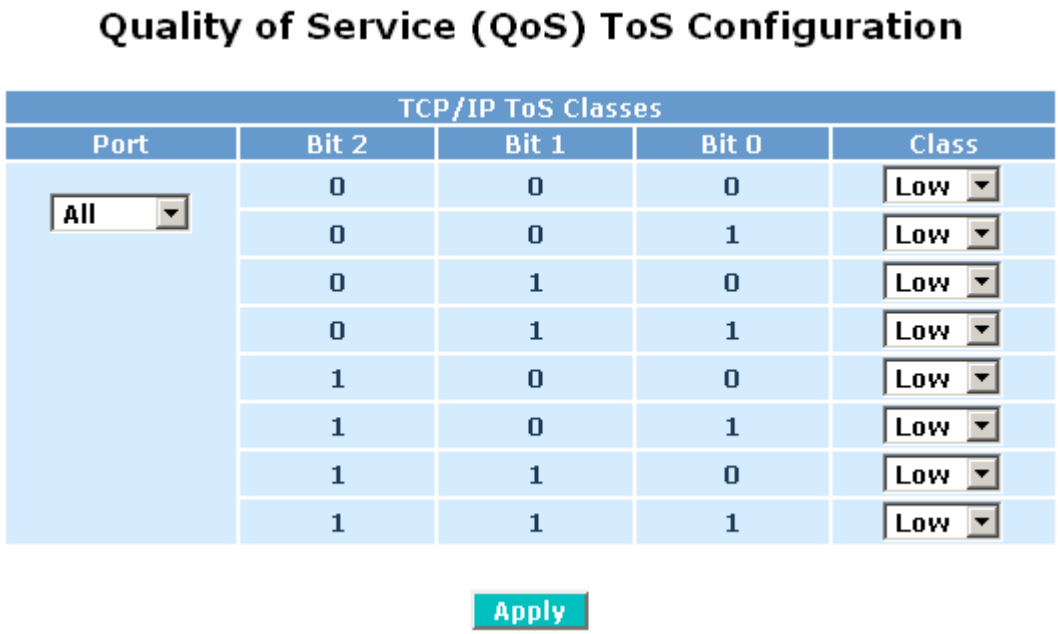

Figure 3-18: Quality of Service ToS Configuraiton

Quality of Service Layer-4 Configuration

Quality of Service Layer-4 Configuration (Figure 3-19) works by prioritizing traffic based on the TCP or UDP port used. For your convenience, there are predefined groups of ports that are commonly used by certain applications. You can also define your own priorities for different port ranges in the advanced mode as well by clicking the “Advance >>” button.

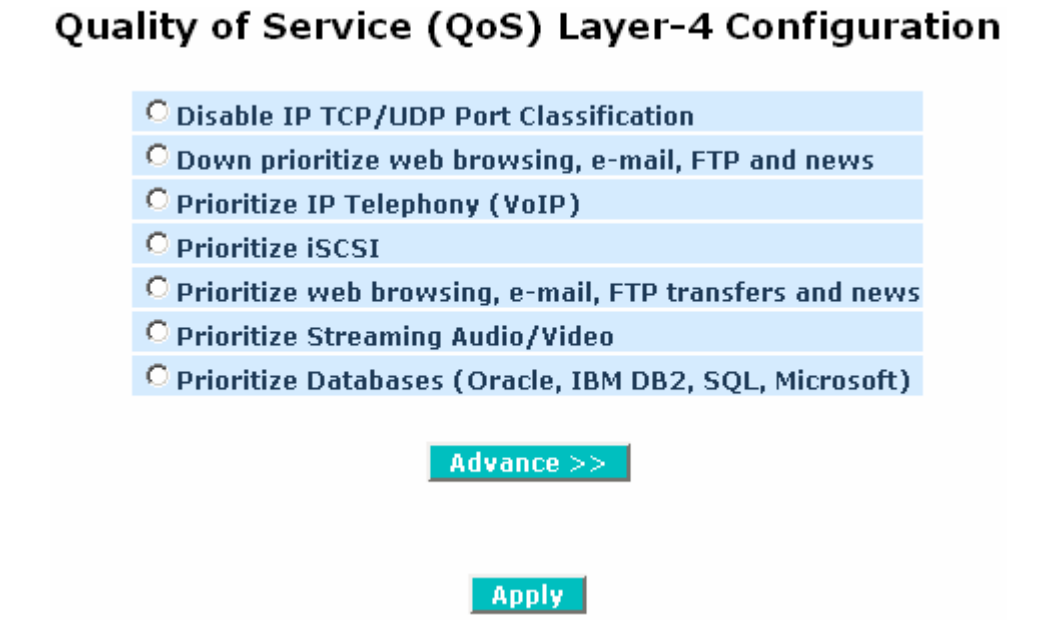
Quality of Service (QoS) Layer-4 Configuration
Disable IP TCP/UDP Port Classification
Down prioritize web browsing, e-mail, FTP and news
Prioritize IP Telephony (VoIP)
Prioritize iSCSI
Prioritize web browsing, e-mail, FTP transfers and news
Prioritize Streaming Audio/Video
Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft)
Advance >>
Apply

Figure 3-19: QoS Simple Mode

Description of options:

Down prioritize web browsing, e-mail, FTP and news sets traffic on ports 80, 280, 443, 25, 110, 20, 21, 69, 119, and 2009 to low priority.

Prioritize IP Telephony (VoIP) sets traffic on ports 1718, 1719, and 1720 to high priority.

Prioritize iSCSI sets traffic on ports 3225, 3260, and 3420 to high priority.

Prioritize web browsing, e-mail, FTP and news sets traffic on ports 80, 280, 443, 25, 110, 20, 21, 69, 119, and 2009 to high priority.

Prioritize Streaming Audio/Video sets traffic on ports 2979, 1755, 7070, 7071, 554, 8000 to high priority.

Prioritize Databases (Oracle, IBM DB2, SQL, Microsoft) sets traffic on ports 66, 1571, 1575, 523, 118, 156, 3306, 1232, 1433, 1434 to high priority.

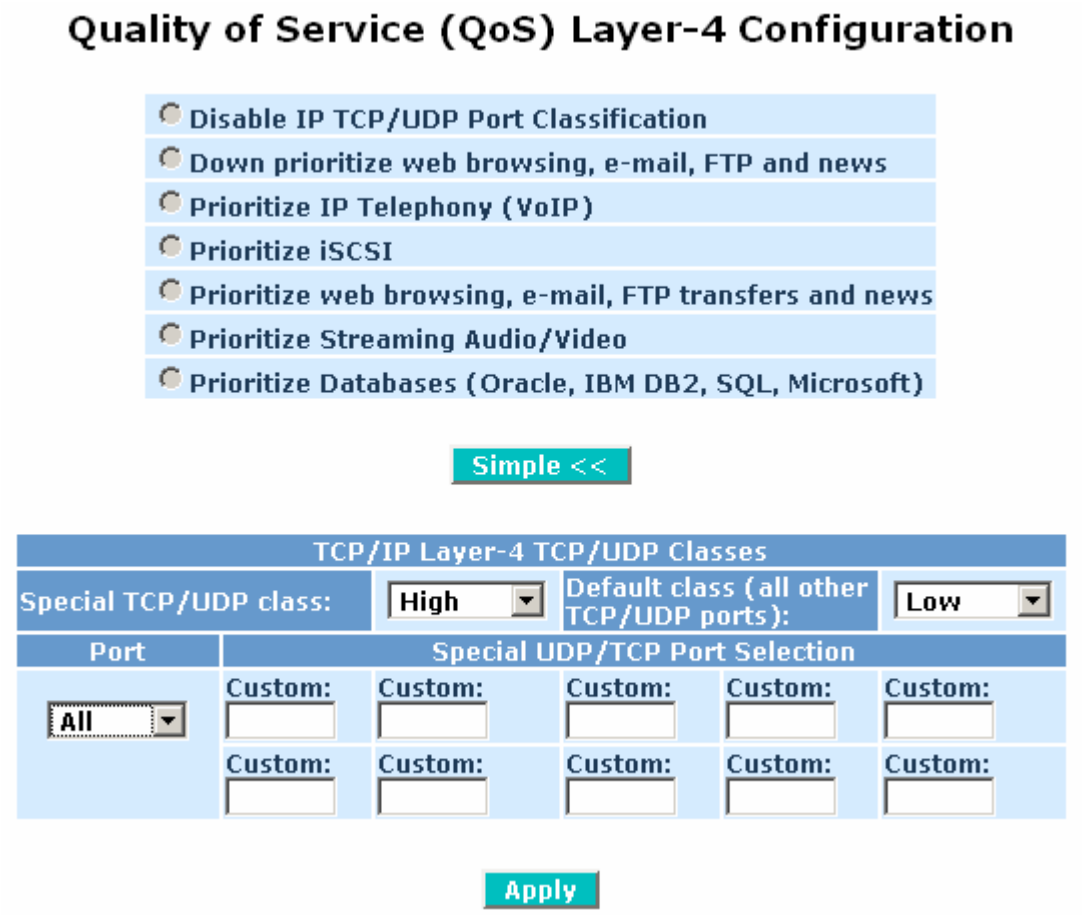

Figure 3-20: QoS Advanced Mode

Advanced Mode (Figure 3-20) allows you select up to ports to prioritize the traffic on (set either to high or low priority), with traffic on the other ports being set to the other priority class.

Special TCP/UDP class: The priority to assign to traffic that is sent on the port(s) defined under Special UDP/TCP Port Selection.

Default class (all other TCP/UDP ports): The priority to assign to traffic that is sent on ports not defined under Special UDP/TCP Port Selection.

Port: The physical port to apply the rules to. If you would like to configure all ports at a time, select “All”.

Special UDP/TCP Port Selection: Select which port(s) to prioritize.

IP DiffServ Classification

IP DiffServ Classification (Figure 3-21) works by prioritizing traffic based on the 8-bit Service Type field in each packet as defined by the IETF for differentiated services. Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

IP DiffServ Classification allows you to select the prioritization level (high or low) based on the DiffServ field value which ranges from 0 to 63. This works similarly to VLAN Tag priority. Click “Apply” to save your settings.

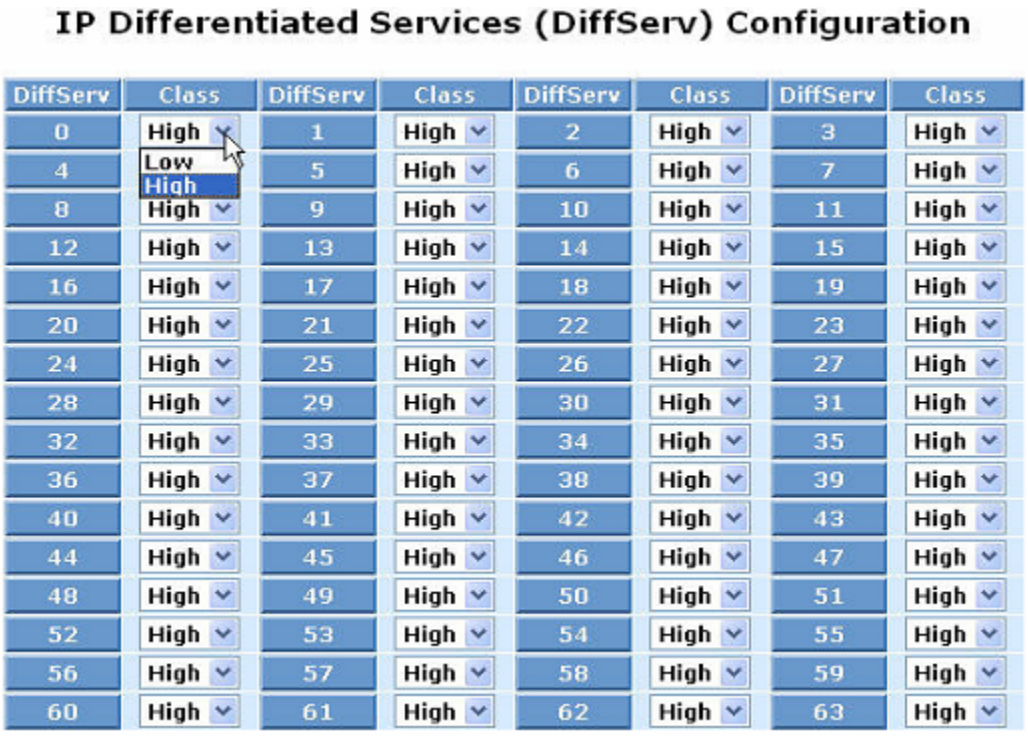

Figure 3-21: IP DiffServ Configuration

3.6 SNMP Configuration

The SNMP Configuration page (Figure 3-23) allows the user to configure the SNMP settings for the switch. Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the switch, provided that the Management Information Base (MIB) is installed correctly on the managing computer. SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the Management Information Base (MIB). An SNMP agent runs on the switch to respond to requests issued by SNMP manager. The SNMP agent is passive, only responding to requests, except for trap information which is sent from the switch.

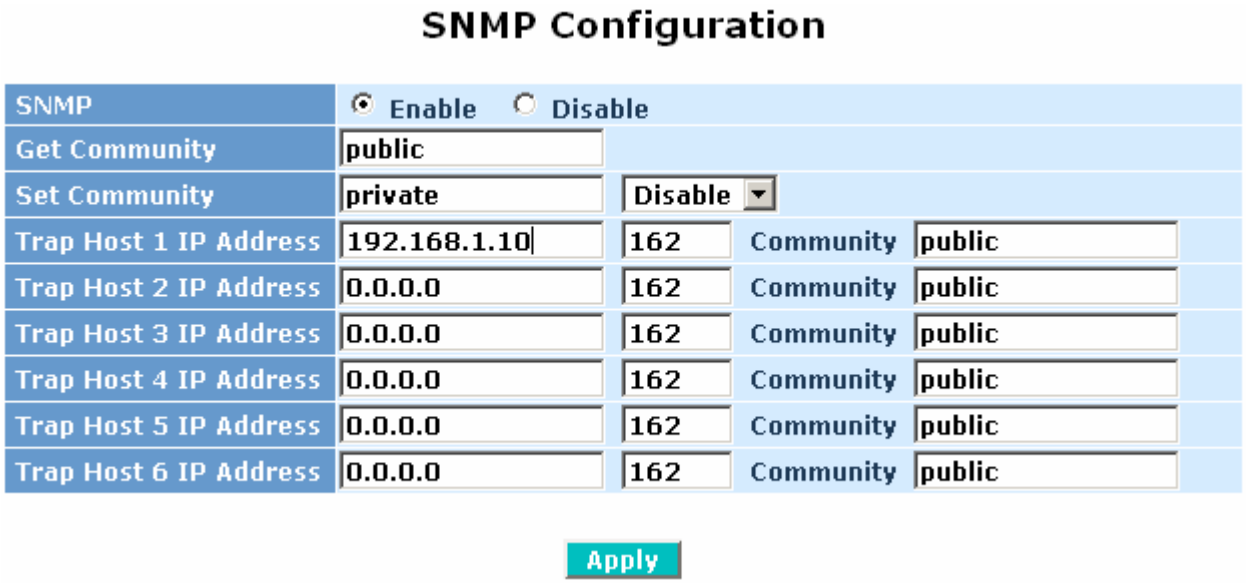

Figure 3-22: SNMP Configuration Page

SNMP: Used to Enable or Disable SNMP. The default is Enable.

Get/Set/Trap Community: The community name is used as password for authentication. The switch will only communicate with the SNMP manager if the community strings are the same. Community name is user-definable with a maximum length of 15 characters and is case sensitive. Any characters other than spaces are allowed.

Each function has its own community name. For example, the community name for GET only works for GET functions and can't be applied to other functions such as SET and Trap.

Set Community can be set to Disable to disallow setting of any switch settings by the SNMP management software. The default is Enable.

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default trap host IP address: 0.0.0.0

Default port number: 162

Trap: The switch supports up to 6 trap hosts, each of them having its own community name, IP address and port. Each host must be running an SNMP management software capable of receiving standard SNMP traps. For each public trap, the switch supports the following trap events: Cold Start, Warm Start, Link Down, Link Up and Authentication Failure Traps. They can be enabled or disabled individually. When enabled, the corresponding trap will send a trap message to the trap host when a trap event occurs. If all public traps are disabled, no public trap message will be sent. The Enterprise trap (number 6) is classified as a private trap, and is listed in the Trap Alarm Configuration folder. The default for all public traps is Enable.

3.7 IGMP Snooping

The IGMP Snooping page (Figure 3-23) is used to establish the multicast groups to forward multicast packets to, thereby avoiding wasting the bandwidth while IP multicast packets are running over the network. Switches that do not support IGMP or IGMP Snooping cannot tell the difference between a multicast packet from the broadcast packet, so it can only treat them all as the broadcast packets. Without

IGMP Snooping, multicast packet forwarding is effectively the same as broadcast packet forwarding.

A switch that supports IGMP Snooping with query, report and leave functions based on a type of packet exchanged between the IP Multicast Router/Switch and IP Multicast Host can update the information in the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this functionality, once a switch receives an IP multicast packet, it will forward the packet to the members who belong to a specified IP multicast group. Multicast packets that a user transmits to a multicast group that had not been defined in advance are discarded.

IGMP is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP in either passive or active mode allows you to monitor the IGMP information which contains the multicast member list with the multicast groups, VID and member ports.

Figure 3-23: IGMP Snooping Page

IGMP snooping mode selection: The switch supports three kinds of IGMP Snooping status, including “Passive”, “Active” and “Disable”.

“Disable” disables IGMP snooping on the switch.

In “Active” mode, the switch will periodically issue a Membership Query message to all hosts attached to it and gather the Membership report message to update the multicast table. Using this method reduces the amount of unnecessary multicast traffic.

In “Passive” mode, switch will not periodically poll the hosts in the groups. The switch will send a Membership Query message to all hosts only when it has received a Membership Query message from a router.

IP Address: Shows all multicast groups’ IP addresses that are registered on this device.

VLAN ID: Shows the VLAN ID for each multicast group.

Member Port: Shows the member ports that have joined each multicast group. Member ports can belong to multiple groups.

3.8 Maximum Packet Length

The Maximum Packet Length page (Figure 3-24) allows you to set the maximum packet size for each port. The switch is capable of handling jumbo frames up to 9kb in size. The default is 1518 for each port.

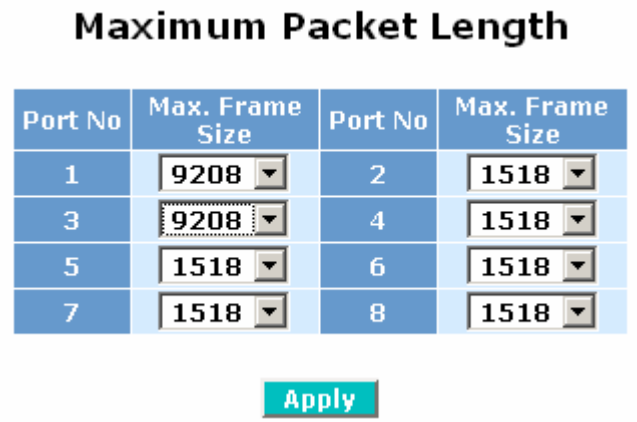

Figure 3-24: Maximum Packet Length Page

3.9 DHCP Boot

The DHCP Boot page (Figure 3-25) allows the user to configure the boot up and DHCP request delay for the switch. Enabling DHCP Broadcast Suppression will cause the switch to delay booting up for between 1 and 30 seconds to avoid overloading the DHCP server with requests in the event of a building-wide power failure. If all of the devices are powered up simultaneously and all request IP addresses using DHCP at the same time, it may cause an overload on the network or on the DHCP server. Delaying the DHCP request using this feature will prevent this from happening.

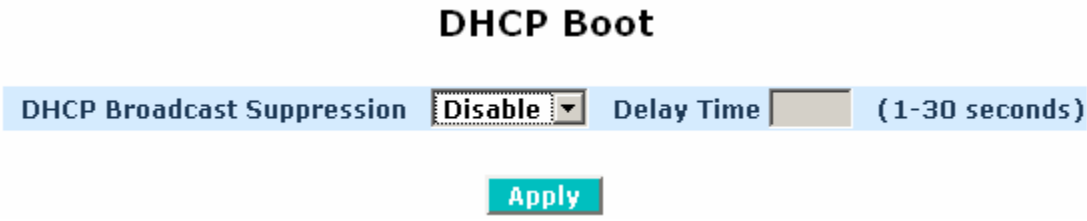

Figure 3-25: DHCP Boot Page

3.10 VLAN

The switch supports both Tag-based VLAN (802.1Q) and Port-based VLAN. It supports 256 active VLANs and VLAN IDs from 1 to 4094. VLANs are used to partition your LAN into smaller ones to prevent different networks from talking to each other, and to limit broadcast domains. Properly configured, VLANs provide improved security and performance on the network.

3.10.1 VLAN Mode

The VLAN Mode page (Figure 3-26) allows the user to select the VLAN mode to use. Five modes are available: Port-based, Tag-based, Metro Mode, Double-tag and Disable. Select the desired mode and then click Apply. The settings will take effect immediately.

VLAN Modes:

Disable: Disable VLANS on the switch. This is the default setting.

Port-based: Port-based VLANs are defined by port. No filtering is applied to the packets on each port, the only limiting factor is that only ports in the same VLAN can communicate with each other. Each port-based VLAN must be assigned a unique group name. The switch can support up to a maximum of 8 port-based VLAN groups.

Tag-based: Tag-based VLANs are identified by its VLAN ID or VID. Instead of filtering by port, all packets coming into and out of the switch are filtered based on the VLAN ID in the packet, and are grouped accordingly. The switch supports 802.1Q tag-based VLANs. Each tag-based VLAN must be assigned a unique VLAN name and VLAN ID. Valid VLAN IDs range from 1 to 4094. Up to 64 VLAN tag groups can be created.

Metro Mode: Metro Mode is a quick configuration that creates 6 or 7 port-based VLAN groups (see below for details).

Double-tag: Double-tag mode is similar to tag-based mode, however it treats all frames as untagged ones, which means that a PVID tag will be added to all packets. Then, these packets will be forwarded using Tag-based VLAN rules. Thus, all incoming packets with tags will become the double-tag packets.

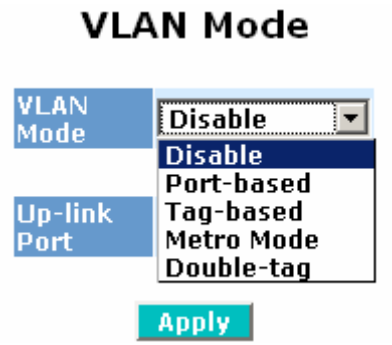

Figure 3-26: VLAN Mode Page

Up-link Port: This section is only enabled when metro mode is chosen as the VLAN mode (Figure 3-27). Possible options are:

7: All ports can only transmit data to and from port 7. This effectively creates 7 port-based VLAN groups between each port and port 7 (1 & 7, 2 & 7, 3 & 7, etc.)

8: All ports can only transmit data to and from port 8. This effectively creates 7 port-based VLAN groups between each port and port 8 (1 & 8, 2 & 8, 3 & 8, etc.)

7&8: All ports can only transmit data to and from ports 7 and 8. This effectively creates 6 port-based VLAN groups between each port and ports 7 and 8 (1 & 7 & 8, 2 & 7 & 8, 3 & 7 & 8, etc.)

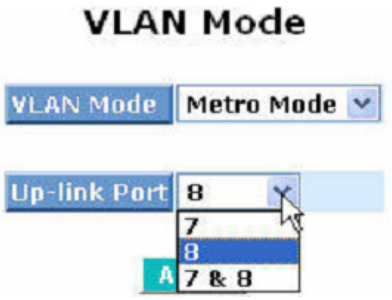

Figure 3-27: Up-link Port Selection

3.10.2 Tag-based Group

The Tag-based Group page (Figure 3-28) allows the user to create, edit, and delete Tag-based VLAN groups. To delete a group, select the VLAN to delete and click the “Delete” button at the bottom of the page.

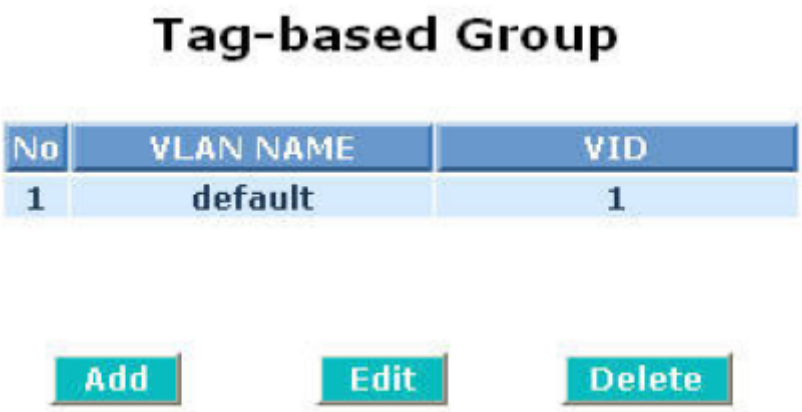

Figure 3-28: Tag-based Group Page

To edit a group, select the group and click the “Edit” button at the bottom of the page. To add a new group, click “Add” at the bottom of the page. Enter the VLAN name as well as the VID, configure the SYM-VLAN and choose the member ports by checking the check boxes beside the desired port numbers, then click the “Apply” to save the settings (Figure 3-29).

Figure 3-29: Add/Edit Tag-based VLAN

VLAN Name: The name associated with the VLAN as defined by the network administrator. Names can be a string up to 15 characters long consisting of letters, numbers, hyphens, and underscores.

VID: The VLAN identifier for the group. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

SYM-VLAN: If the SYM-VLAN function of the group is enabled, all packets with this group VID will be dropped if they are transmitted from the ports that do not belong to this group.

Member: Select which ports belong to the VLAN be selecting the check boxes beside each port.

3.10.3 Port-based Group

The Port-based Group page (Figure 3-30) allows the user to create, edit, and delete port-based VLAN groups. To delete a group, select the VLAN to delete and click the “Delete” button at the bottom of the page.

Figure 3-30: Port-based Group Page

To edit a group, select the group and click the “Edit” button at the bottom of the page. To add a new group, click “Add” at the bottom of the page. Enter a VLAN name and choose the member ports by checking the check boxes beside the desired port numbers, then click the “Apply” to save the settings (Figure 3-31). VLAN names can be a string up to 15 characters long consisting of letters, numbers, hyphens, and underscores.

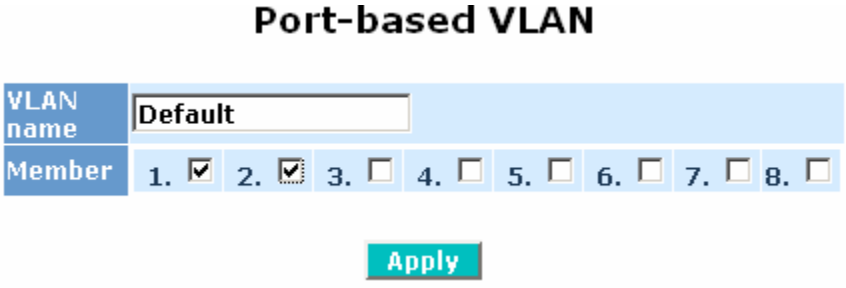

Figure 3-31: Add/Edit Port-based VLAN

3.10.4 Tag Rule

The Tag Rule page (Figure 3-32) allows the user to set the VID number for each port. The range of VID numbers is from 1 to 4094. The user can also choose ingress filtering rules for each port. There are two ingress filtering rules which can be applied to the port. Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”. Ingress Filtering Rule 2 is “drop untagged frame”. You can also select the Role of each port as Access, Trunk, or Hybrid.

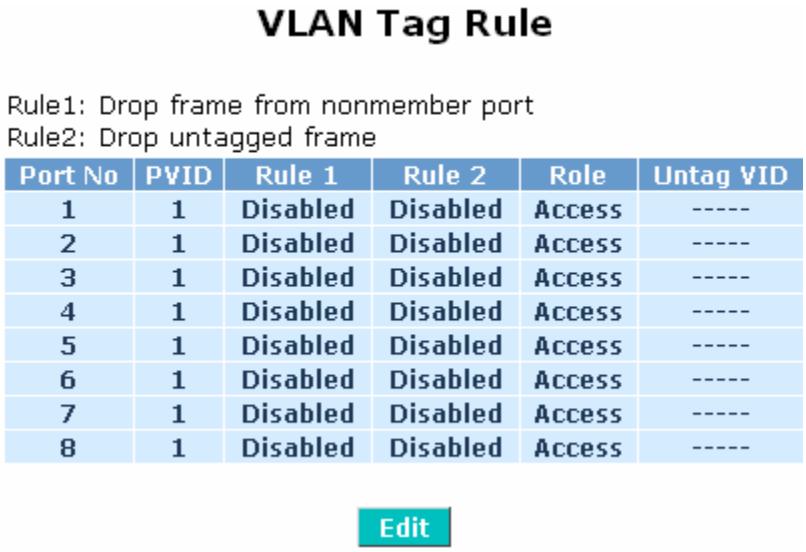
VLAN Tag Rule
Rule1: Drop frame from nonmember port
Rule2: Drop untagged frame
Port No PVID Rule 1 Rule 2 Role Untag VID
1 1 Disabled Disabled Access -----
2 1 Disabled Disabled Access -----
3 1 Disabled Disabled Access -----
4 1 Disabled Disabled Access -----
5 1 Disabled Disabled Access -----
6 1 Disabled Disabled Access -----
7 1 Disabled Disabled Access -----
8 1 Disabled Disabled Access -----
Edit

Figure 3-32: VLAN Tag Rule Page

Port No: Port number.

PVID: The PVID range is between 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as a tagged packet with VID y.

Rule 1: Forward only packets with VID matching this port's configured VID. You can apply Rule 1 to a given port to filter unwanted traffic. Using Rule 1, a given port checks if the destination port is a member of the VLAN to which the received packet belongs to in order to determine whether to forward it or not. For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Rule 1 is enabled, the switch will check if port 1 is a member of VLAN100. If it is, the received packet is forwarded; otherwise, the received packet is dropped.

Rule 2: Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frames. If the former is the case, then tagged and untagged packets will be processed. If the latter is the case, only packets containing VLAN tags will be processed, the rest of the packets will be discarded.

> **Example:** If Rule 1 is enabled and port 1 receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet will then will be forwarded. But if the PVID of port 1 is 100 and port 1 is not a member of VLAN 100, the packet will be dropped.

Role: This is an egress rule for the port. The available options are Access, Trunk or Hybrid. Trunk means that outgoing packets must carry a VLAN tag header. Access means that outgoing packets carry no VLAN tag header. If packets have double VLAN tags, one will be dropped and the other will still be left. Hybrid is similar to Trunk, in that both of them will send tags out. However, when the port is set to Hybrid, its packets will be untagged out if the VID of the outgoing packet with tags is the same as the one in the Untag VID field for this port.

Untag VID: Valid range is 1-4094. Only used when Role is set to Hybrid.

3.11 MAC Table

The MAC Table menu provides different functions for viewing and managing the MAC address table on the switch. The different pages are describe in detail in the following sections.

3.11.1 Information

The Information page (Figure 3-33) displays the current MAC address table in the switch including static and dynamic MAC entries.

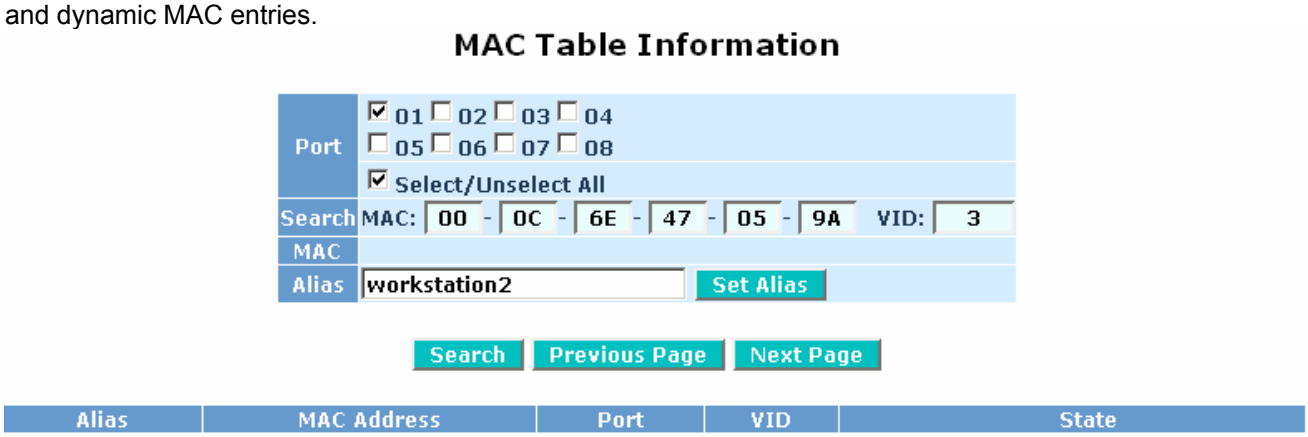

Figure 3-33: MAC Table Information Page

Port: Select the port you would like to filter by.

Search: Search by a specific MAC address or VID.

MAC: Display the MAC address of the entry you selected from the search results. Used for Set Alias.

Alias: Create an alias for the selected MAC entry. Click “Set Alias” to save.

Search: Find entries that meet the criteria.

Previous Page: Move to the previous page.

Next Page: Move to the next page.

Search results:

Alias: The alias of the entry.

MAC Address: The MAC address of the entry.

Port: The port associated to the MAC address.

VID: The VLAN Group for the MAC entry.

State: The method that this MAC entry was entered, either “Dynamic MAC” or “Static MAC”.

3.11.2 Maintenance Page

The Maintenance page (Figure 3-34) allows the user to set the aging time for dynamic MAC address entries, and flush all dynamic MAC address entries.

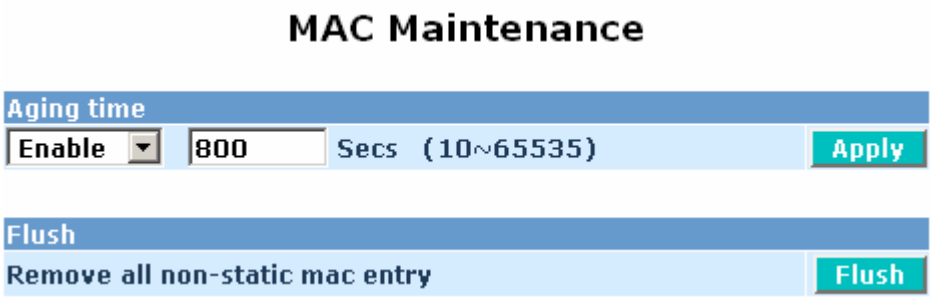

Figure 3-34: MAC Table Maintenance Page

Aging Time: An idle MAC address that has exceeded the MAC address aging time will be removed from the MAC address table. This setting has no effect on static MAC address. Range for Aging Time is from 10-65535 seconds. The default is 300 seconds.

Flush: Remove all entries that are not static MAC entries from the MAC address table.

3.11.3 Static Forward

The Static Forward page (Figure 3-35) allows the user to add or remove static MAC addresses from the MAC address table. The static forward table associates a MAC address with a port and VID. When a MAC address is assigned to a specific port, all of the traffic sent to this MAC address will be forwarded to specified port.

To add a MAC address entry in the table, fill in the four parameters: MAC address, associated port, VID and Alias, and click “Add”. To delete an entry, select the MAC address entry you wish to delete and click “Delete”.

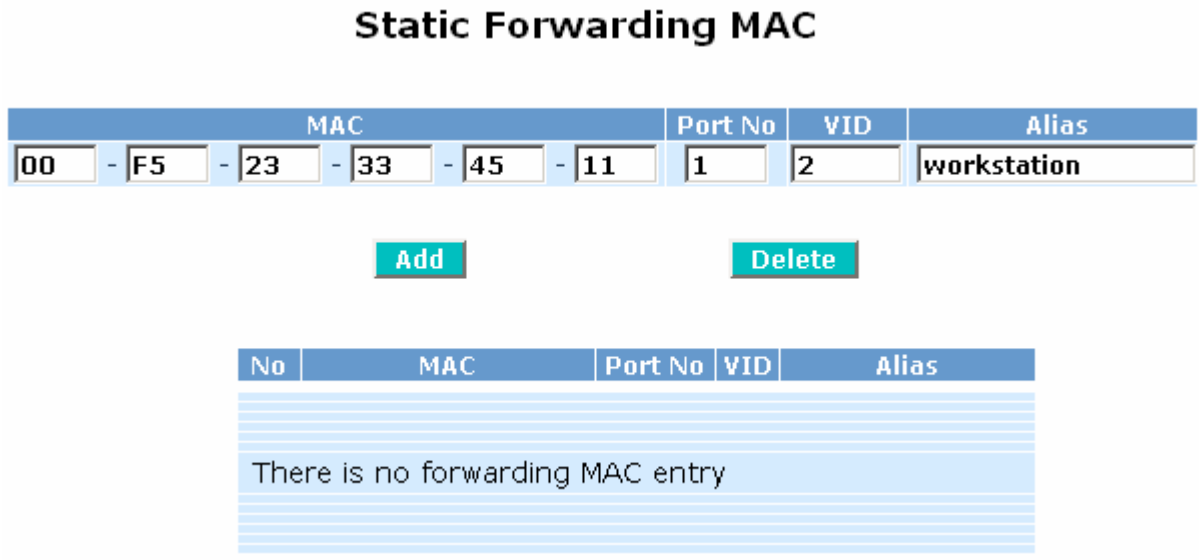

Figure 3-35: Static Forward Page

MAC: A six-byte long Ethernet hardware address and expressed in hex and separated by hyphens.

Port No: Port number of the switch between 1-8.

VID: VLAN identifier. This only applies if tagged VLANs are enabled. Valid range is from 1-4094.

Alias: Alias name for the MAC address.

3.11.4 Static Filter

The Static Filter page (Figure 3-36) allows the user deny packet forwarding to specific MAC addresses. The static filter table contains a MAC address and VID. All of the traffic sent to this MAC address will be discarded by the switch.

To add a MAC address entry in the table, fill in the three parameters: MAC address, VID and Alias, and click “Add”. To delete an entry, select the MAC address entry you wish to delete and click “Delete”.

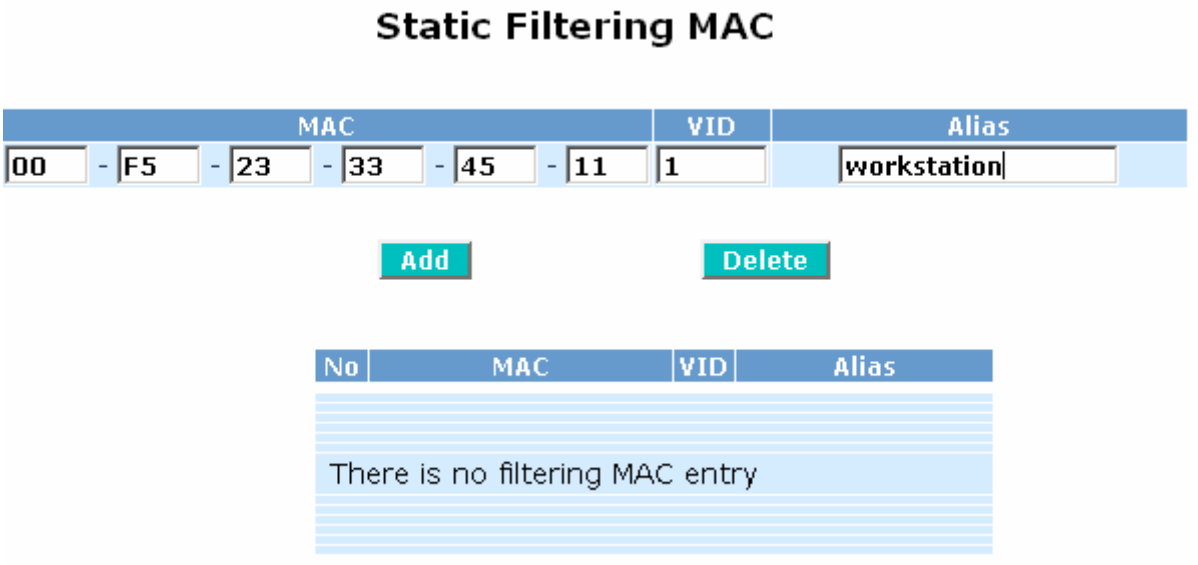

Figure 3-36: Static Filter Page

MAC: A six-byte long Ethernet hardware address and expressed in hex and separated by hyphens.

VID: VLAN identifier. This only applies if tagged VLANs are enabled. Valid range is from 1-4094.

Alias: Alias name for the MAC address.

3.11.5 MAC Alias

The MAC Alias page (Figure 3-37) is used to allows the user to assign a plain English name to a MAC address. This will help you tell which MAC address belongs to which user in the illegal access report.

To create or edit an entry, enter the MAC address and alias name and click “Create/Edit”. To delete an entry, select it from the list and click “Delete”. The alias name must be composed of only letters and number and can be up to 15 characters long.

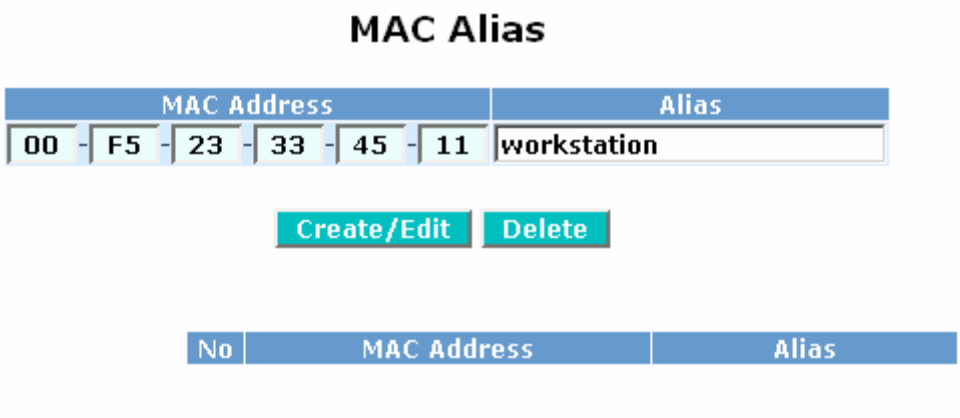

Figure 3-37: MAC Alias Page

MAC: A six-byte long Ethernet hardware address and expressed in hex and separated by hyphens.

Alias: Alias name for the MAC address.

> **Note:** If there are too many MAC addresses in the table, it is recommended that you input the MAC address and alias name manually.

3.12 GVRP Configuration

GVRP is an application based on Generic Attribute Registration Protocol (GARP) mainly used to automatically and dynamically maintain the group membership information of VLANs. GVRP provides the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, the GVRP state machine maintains the contents of Dynamic VLAN Registration Entries for each VLAN and propagates this information to other GVRP-aware devices to setup and update their knowledge database including the set of VLANs associated with currently active members, and through which ports these members can be reached.

In the GVRP Configuration function folder, there are three functions supported, GVRP Config, GVRP Counter and GVRP Group, which are explained in detail in the following sections.

3.12.1 Config

The Config page (Figure 3-38) is used to configure each port's GVRP operation mode, as described below.

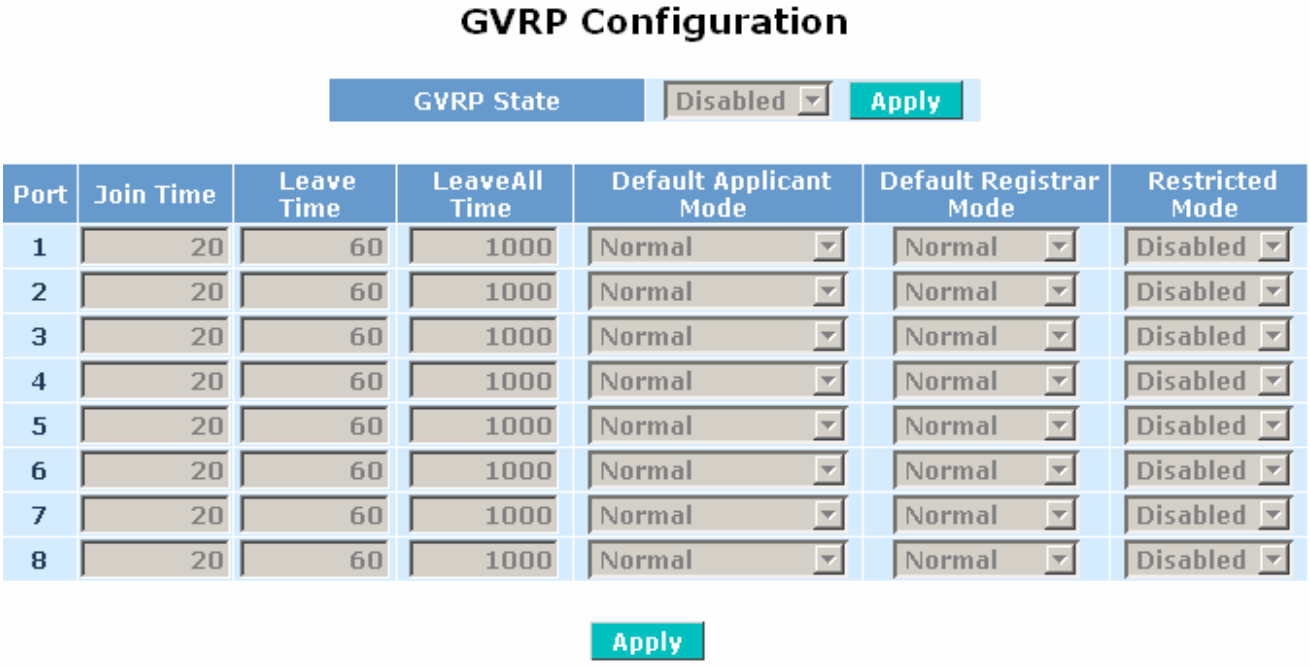

Figure 3-38: GVRP Configuration Page

GVRP State: Allows you to enable or disable GVRP.

Join Time: The Join Time in centiseconds (one hundredths of a second). Valid time range is between 20-100, default is 20.

Leave Time: The Leave Time in centiseconds. Valid time range is between 60-300, default is 60.

Leave All Time: A time period for announcements that all registered devices are going to be de-registered. If someone issues a new join, then the registration will be kept in the switch. Valid range is from 1000-5000, default is 1000.

Default Applicant Mode: Sets the type of participant, either normal participant or non-participant. In normal mode, the switch participates normally in GARP protocol exchanges. In non-participant mode, the switch does not send or reply to any GARP messages. It just listens to messages and reacts to the received GVRP BPDU. The default setting is Normal.

Default Registrar Mode: Sets the type of registrar, either normal registrar, fixed registrar and forbidden registrar. In normal mode, the registrar responds normally to incoming GARP messages. In fixed mode, the Registrar ignores all GARP messages, and all members remain in the registered (IN) state. In forbidden mode, the registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state. The default setting is Normal.

Restricted Mode: Used to restrict dynamic VLANs from being created when this port receives a GVRP PDU. If disabled, the switch's dynamic VLAN will be created when this port received a GVRP PDU. If enabled, the switch does not create dynamic VLANs when this port receives a GVRP PDU, except if it receives dynamic VLAN messages in the GVRP PDU that correspond to an existing static VLAN in the switch, this port will then be added into the static VLAN members. The default setting is Disabled.

3.12.2 Counter

The Counter page (Figure 3-39) displays the GVRP packets sent and received by the switch.

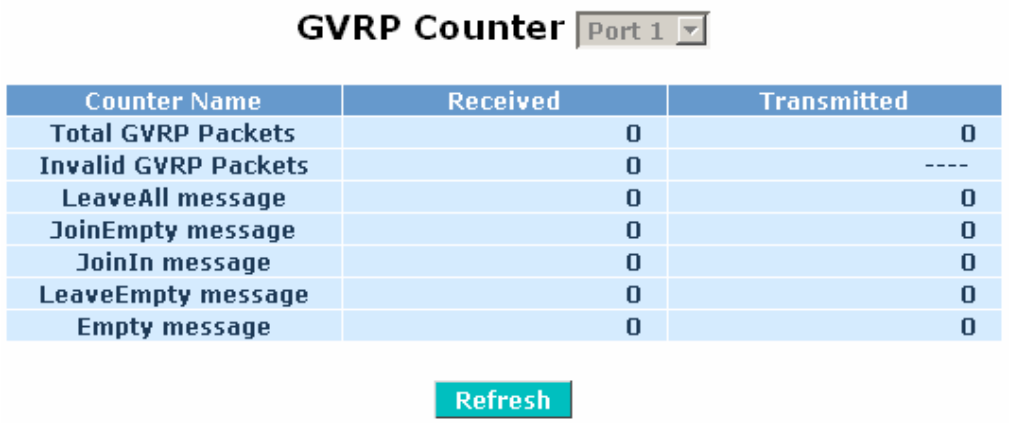

Figure 3-39: GVRP Counter Page

Total GVRP Packets: Total GVRP BPDU packets sent or received by the switch.

Invalid GVRP Packets: Number of invalid GARP BPDU received by the switch.

LeaveAll Message Packets: Number of GARP BPDU with a Leave All message sent or received by the switch.

JoinEmpty Message Packets: Number of GARP BPDU with a Join Empty message sent or received by the switch..

JoinIn Message Packets: Number of GARP BPDU with a Join In message sent or received by the switch.

LeaveEmpty Message Packets: Number of GARP BPDU with a Leave Empty message sent or received by the switch.

Empty Message Packets: Number of GARP BPDU with an Empty message sent or received by the switch.

3.12.3 Information

The Information page (Figure 3-40) displays the dynamic group members and their information.

Figure 3-40: GVRP Group Information

VID: VLAN identifier. Each dynamic VLAN group created by GVRP has its own VID. Valid range is from 1-4094.

Member Port: Those are member ports belonging to the same dynamic VLAN group.

Edit Administrative Control: When you create a GVRP group, you can use Administrative Control to change the Applicant Mode and Registrar Mode of a GVRP group member.

Refresh: Refreshes the current GVRP group status.

3.13 STP Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, the switch ensures that only one path is active between any two nodes on the network at a time. It is recommended that you enable STP on all switches to ensure a single active path on the network.

3.13.1 STP Status

The STP Status page (Figure 3-41) displays the current STP status on the switch.

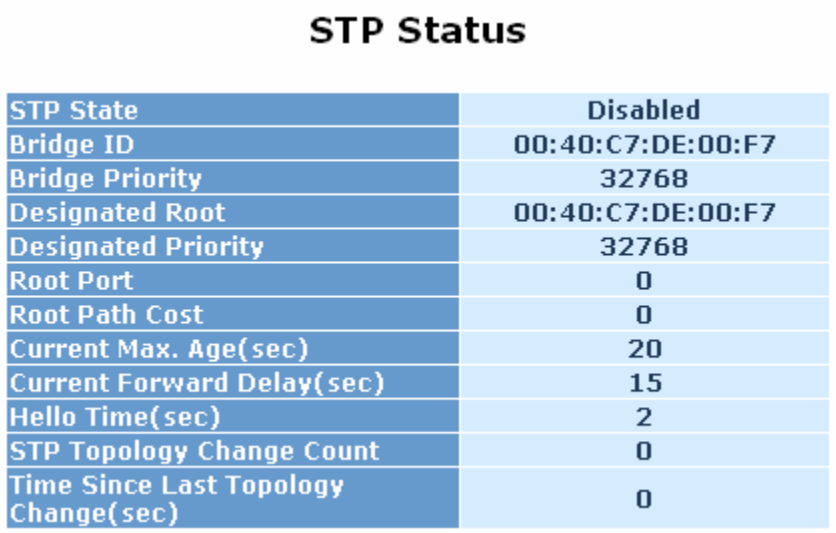

Figure 3-41: STP Status Page

STP State: Shows whether STP is enabled or disabled.

Bridge ID: Shows the switch's bridge ID which is the MAC address of this switch.

Bridge Priority: Shows this switch's current bridge priority setting. Default is 32768.

Designated Root: Shows the root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will be the same as this switch's bridge ID.

Designated Priority: Shows the current root bridge priority.

Root Port: Shows the port number connected to root bridge with the lowest path cost. Will be 0 if the current switch is the root.

Root Path Cost: Shows the path cost between the root port and the designated port of the root bridge. Will be 0 if the current switch is the root.

Current Max. Age: Shows the current root bridge maximum age time. The maximum age time is used to monitor if the STP topology needs to change. When a bridge does not receive a hello message from the root bridge before the maximum age time counts down to 0, the bridge will treat the root bridge as unavailable and will issue a Topology Change Notification (TCN) BPDU to all other bridges. At this time, all bridges in the LAN will re-learn and determine which switch is the new root bridge. Maximum Age time is assigned by the root bridge. Default is 20 seconds.

Current Forward Delay: Shows the current root bridge forward delay time. The value of Forward Delay time is set by the root. The Forward Delay time is defined as the time spent from Listening state moving to Learning state or from Learning state moving to Forwarding state of a port in a bridge.

Hello Time: Shows the current hello time of the root bridge. Hello time is a time interval specified by the root bridge used to request that all other bridges periodically send hello message every "hello time"

seconds to the bridge attached to its designated port.

STP Topology Change Count: Shows the time spent in seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change has converged, the Topology Change count will be reset to 0.

Time Since Last Topology Change: Shows the accumulated time in seconds since the last STP Topology Change was made. When a Topology Change is initiated again, this counter will be reset to 0. It will start counting again once the STP Topology Change is completed.

3.13.2 Configuration

The STP Configuration page (Figure 3-42) allows the user to set the STP settings for the switch. The settings are described below.

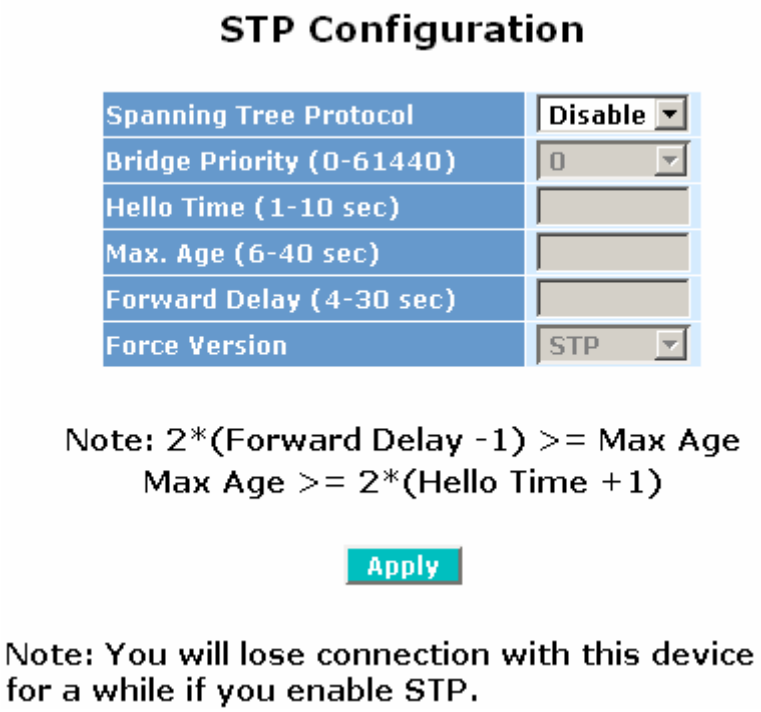

Figure 3-42: STP Configuration Page

Spanning Tree Protocol: Sets whether 802.1w Rapid STP function is enabled or disabled. Default is Disable.

Bridge Priority: The lower the bridge priority, the higher the priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the SS2GD8I as the root bridge, you should set this value lower than that of the other bridges in the LAN. Valid values are from 0-61440. The default is 32768.

Hello Time: Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how often a bridge should send this message to other bridges saying that it is active. When the SS2GD8I is the root bridge, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. Valid values are from 1-10 seconds. Default is 2 seconds.

Max. Age: When the SS2GD8I is the root bridge, all other switch on the LAN will use this number as their maximum age time. When a bridge receives a BPDU originating from the root bridge and if the message age conveyed in the BPDU exceeds the max. age of the root bridge, the bridge will treat the root bridge as unavailable and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will then re-calculate and determine who the new root bridge is. Valid values are from 6-40

seconds. Default is 20 seconds.

Forward Delay: Set the root bridge forward delay time. This figure is set by the root bridge only. The forward delay time is defined as the time spent from Listening state moving to Learning state and also from Learning state moving to Forwarding state of a port in a bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. Assuming that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This affects STP convergent time which will be more than 30 seconds because some other factors. Valid values are from 4-30 seconds, default is 15 seconds.

Force Version: Both RSTP and STP are supported. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (802.1w) which is backwards compatible with STP (802.1d).

3.13.3 Port

The STP Port Configuration page (Figure 3-43) allows the user to configure STP settings for each port. You can disable and enable each port, and also set “Path Cost”, “Priority”, “Admin Edge Port” and “Admin Point To Point” for each port.

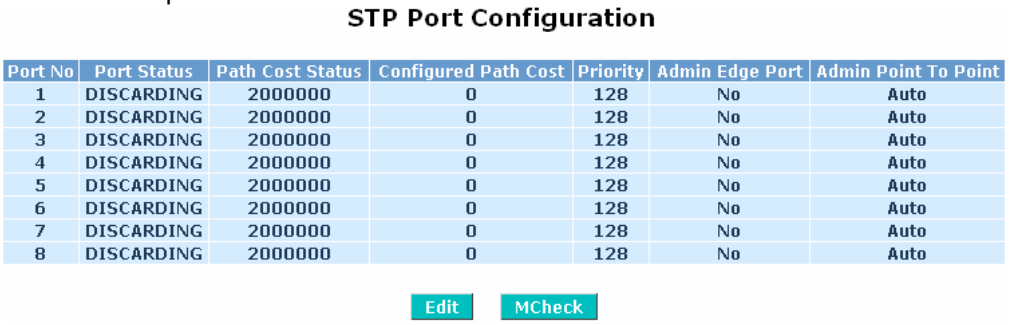
STP Port Configuration
Port No
Port Status
Path Cost Status
Configured Path Cost
Priority
Admin Edge Port
Admin Point To Point
1 DISCARDING 2000000 0 128 No Auto
2 DISCARDING 2000000 0 128 No Auto
3 DISCARDING 2000000 0 128 No Auto
4 DISCARDING 2000000 0 128 No Auto
5 DISCARDING 2000000 0 128 No Auto
6 DISCARDING 2000000 0 128 No Auto
7 DISCARDING 2000000 0 128 No Auto
8 DISCARDING 2000000 0 128 No Auto
Edit
MCheck

Figure 3-43: STP Port Configuration Page

Port Status: Displays the current state of a port as defined by 802.1w.The three states are:

- Discarding state indicates that this port can neither forward packets nor contribute learning knowledge. Note that three other states (disable state, blocking state and listening state) defined in the 802.1d specification are now all represented as the discarding state.
- Learning state indicates that this port can now contribute its learning knowledge but cannot forward packets.
- Forwarding state indicates this port can both contribute its learning knowledge and forward packets normally.

Path Cost Status: Shows the contribution value of the path through this port to the root bridge. The STP algorithm determines a best path to Root Bridge by calculating the sum of path costs contributed by all ports on this path. A port with a smaller path cost value is more likely to become the Root Port.

Configured Path Cost: In the switch, if path cost is set to be zero, STP will get the recommended value resulting from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value entered in the Configured Path Cost and Path Cost Status. Valid range is from 0-200,000,000. Default is 0.

The 802.1w RSTP recommended value depends on the speed of the network. 10 Mbps is 2,000,000, 100 Mbps is 200,000, and 1 Gbps is 20,000.

Priority: Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge will become the Root Port. Valid values are from 0-240. Default is 128.

Admin Edge Port: If “Yes” is selected, this port will be an edge port. An Edge Port is a port connected to

a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology remains unchanged. Unlike the designated port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU. Default is No.

Admin Point To Point: A port is a point-to-point link if it is in full-duplex mode but is a shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port quickly transit to the forwarding state.

There are three option, auto, true and false, used to configure the type of the point-to-point link. If it is set to auto, it means that RSTP will use the duplex mode resulting from auto-negotiation. This is the safest method because although most links run in full-duplex mode, auto-negotiation may set it to half-duplex. If it is set to true, the port will be treated as a point-to-point link and unconditionally transit to the forwarding state. If it is set to false, fast transition to forwarding state will not happen on this port. Default: Auto

M Check: Stands for Migration Check. Forces the port to send out an RSTP BPDU instead of a legacy STP BPDU during the next transmission. The only benefit of this operation is to make the port quickly revert to act as an RSTP port. Click the “M Check” button to send a RSTP BPDU from the specified port.

3.14 Trunking Configuration

The Port Trunking Configuration is used to configure the link aggregation settings on the switch. With link aggregation, you can group multiple ports together that have the same speed, are full duplex and have the same MAC address to be a single logical port, thus the combining the bandwidth of these ports. For example, if there are three Fast Ethernet ports aggregated together into one logical port, then this logical port has a bandwidth three times faster than a single Fast Ethernet port.

The switch supports two types of port trunking methods:

LACP: Ports using Link Aggregation Control Protocol (according to the IEEE 802.3ad specification) as their trunking method can choose their unique LACP Group ID (1-8) to form a logical “trunked port”. The benefit of using LACP is that a port has to negotiate with its peer’s ports before it becomes a member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method, static trunks.

LACP does not support the followings:

- Link Aggregation across switches.
- Aggregation with non-IEEE 802.3 MAC links.
- Operating in half-duplex mode.
- Aggregating ports with different data rates.

Static Trunk: Ports using Static Trunk as their trunk method can choose their unique Static Group ID (also 1~8, this Static groupID can be the same with another LACP group ID) to form a logical “trunked port”. The benefit of using Static Trunk is that a port can immediately become a member of a trunk group without any handshaking with its peer. This is also a disadvantage because the peer ports connect to the static trunk group may not know that they should be aggregated together to. Using Static Trunk on both ends of a link is strongly recommended. Please also note that low speed links will be in a “not ready” state when using static trunk to aggregate with high speed links.

The switch supports 8 “real trunked” groups. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with one or zero ready member-ports is not a “real trunked” group. Any Static trunk group is a “real trunked” group. Each Trunking Group supports a maximum of 12 ready member-ports. Please note that some decisions will automatically be made by the system while you are configuring your trunking ports in order to conform to the rules of 802.3ad.

3.14.1 Port

The Trunk Port Setting/Status page (Figure 3-44) is used to configure the trunk setting of each port in the switch.

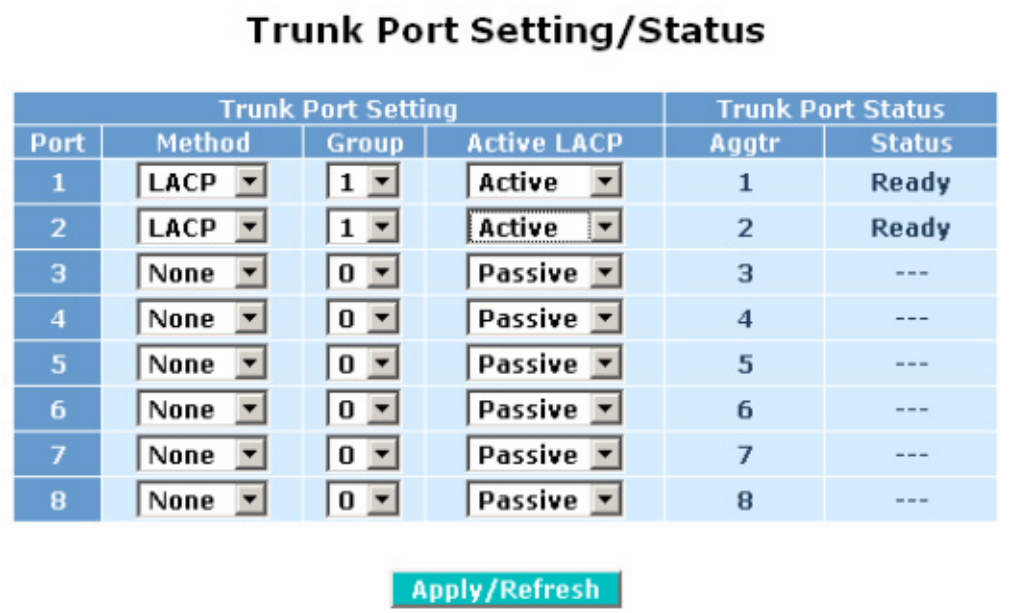

Figure 3-44: Trunk Port Setting/Status Page

Method: Determines the method a port uses to aggregate with other ports. “None” means the port does is not aggregated with any other port. “LACP” means the port is using LACP as its trunk method to become aggregated with other ports also using LACP. “Static” means the port is using Static Trunk as its trunk method to become aggregated with other ports also using Static Trunk.

Group: Ports using the same trunking method other than “None” must be assigned the same unique Group number in order to declare that they wish to aggregate with each other. Valid values are from 1 to 8.

Active LACP: This is used when a port’s trunking method is LACP. An “Active” LACP port begins to send LACPDU to its link partner right after the LACP protocol entity starts to take control of this port. A “Passive” LACP port will not actively send LACPDU out until it receives an LACPDU from its link partner.

Aggtr: Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. The aggregator is the main port for each trunk. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.

Status: Represents the trunking status of a port which uses a trunking method other than “None”. It also represents the management link status of a port which uses the “None” trunking method. “---“ means “not ready”.

3.14.2 Aggregator View

The Aggregator View page (Figure 3-45) displays the current port trunking status.

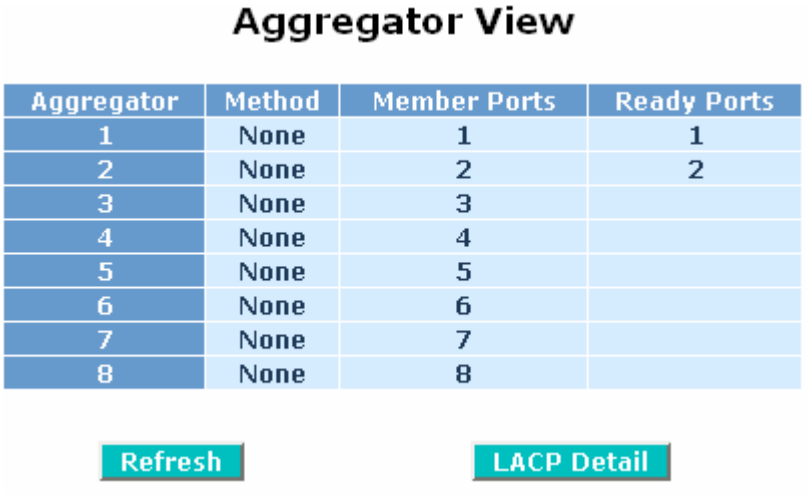

Figure 3-45: Aggregator View Page

Aggregator: Shows the aggregator ID (from 1 to 8) of each port, which is the same as the port number.

Method: Shows the method a port is using to aggregate with other ports.

Member Ports: Shows all of the member ports of an aggregator port.

Ready Ports: Shows only the ready member ports within an aggregator port.

Refresh: Refreshes the information on the screen.

LACP Detail: Clicking this will open a new window showing detailed information on the LACP trunking group (Figure 3-46).

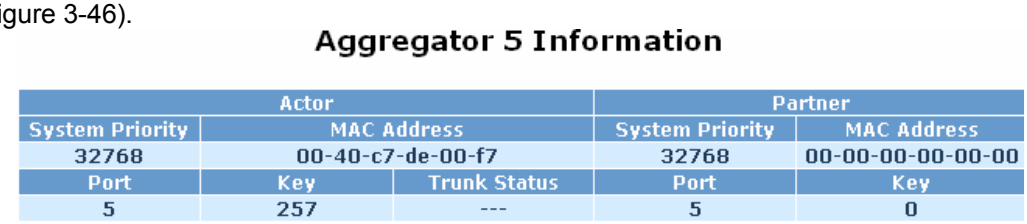

Figure 3-46: LACP Detail Page

Actor: The switch you are watching on.

Partner: The peer system.

System Priority: Shows the System Priority part of a system ID.

MAC Address: Shows the MAC Address part of a system ID.

Port: Shows the port number part of an LACP port ID.

Key: Shows the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set manually.

Trunk Status: Shows the trunk status of a single member port. "---" means "not ready".

3.14.3 System Priority

The System Priority page (Figure 3-47) is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supporting LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value. The System Priority can be set

manually. The valid range is from 1 to 65535. Default is 32768.

Figure 3-47: LACP System Priority Page

3.15 802.1X Configuration

802.1X port-based network access control provides a method to restrict users from accessing network resources by authenticating the user's information beforehand. This restricts users from gaining access to network resources through a 802.1X-enabled port without authentication. If users wish to access the network through a port under 802.1X control, they must input their account name for authentication and wait for authorization first.

The SS2GD8I only supports multi-host 802.1X authentication. In this mode, the devices connected to a port can only gain access to the network through this port after it has been authorized.

3.15.1 State

The 802.1X State Setting page (Figure 3-48) is used to configure the global parameters for RADIUS authentication to authenticate for 802.1X port security.

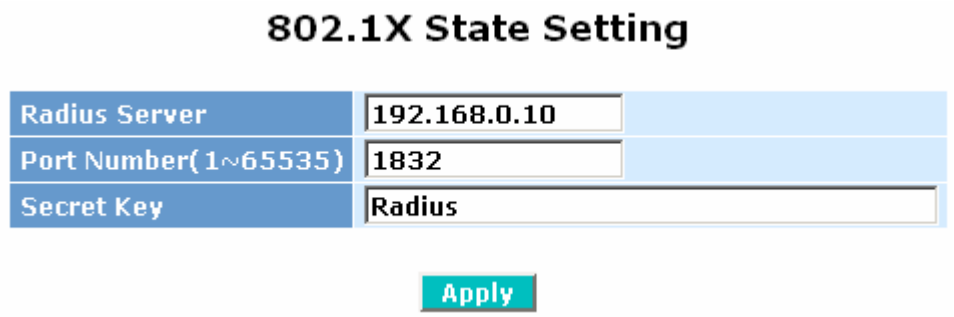

Figure 3-48: 802.1X State Setting Page

Radius Server: RADIUS server IP address for authentication. Default is 192.168.1.1

Port Number: The port number used to communicate with the RADIUS server. Valid value ranges from 1-65535. Default port number is 1812.

Secret Key: The secret key between authentication server and authenticator. It is a string up to 31 characters long. The string may contain only letters and numbers, and is case sensitive. Default is "Radius".

3.15.2 Mode

The 802.1X Mode Setting page (Figure 3-49) sets the operation mode of 802.1X for each port. Only multi-host operation mode is supported.

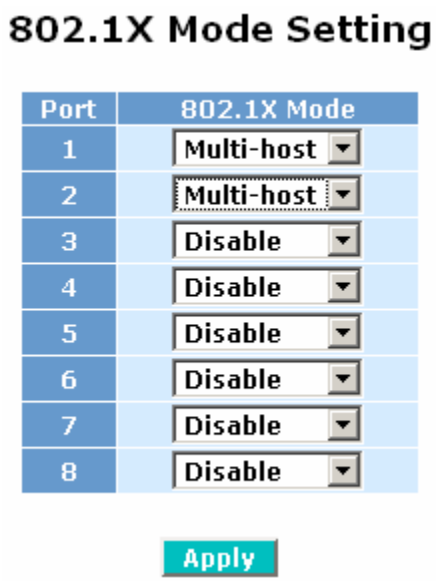

Figure 3-49: 802.1X Mode Setting Page

Port Number: Port number to configure.

802.1X Mode: 802.1X operation mode. Can either be “Disable” and “Multi-host” mode. In disable mode, no authentication is performed. In multi-hose mode, all supplicants must be authorized before connecting to the network. Default is Disable.

3.15.3 Security

The Port Security Management page (Figure 3-50) shows the status of each port. In Multi-host mode, it shows the port number and its status, either authorized or unauthorized.

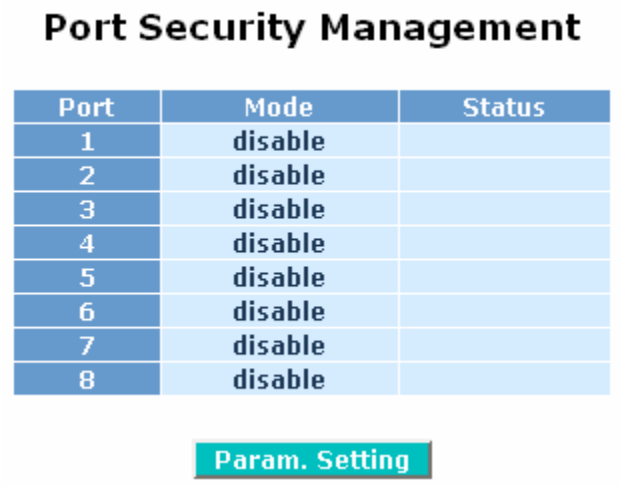

Figure 3-50: Port Security Management Page

Port Number: The port number can be selected to show its 802.1X port status by clicking Param. Setting.

Mode: Shows whether the port has 802.1X disabled or is using multi-host mode.

Status: The current 802.1X status of the port, either Authorized or Unauthorized. In Disable mode, this field is blank.

Param. Setting: Selecting a port and clicking the Parameter Setting button will open a new window that

allows you to configure 802.1X details for the port (Figure 3-51).

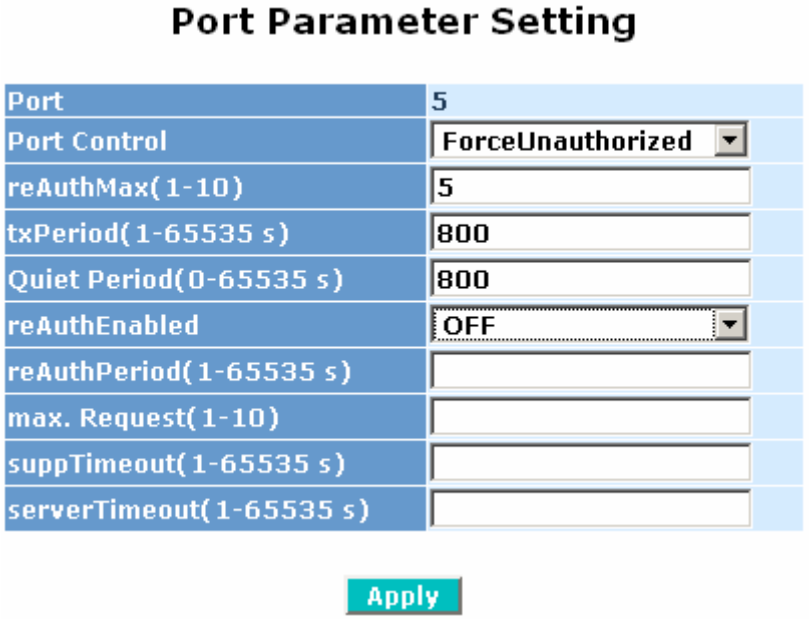

Figure 3-51: Parameter Setting Page

Port: Port number being modified.

Port Control: Used to set the operation mode for authorization. There are three modes supported, ForceUnauthorized, ForceAuthorized, Auto. ForceUnauthorized means the controlled port is always in the unauthorized state. ForceAuthorized means the controlled port is always in the authorized state. Auto means that the controlled port is set to be in authorized state or unauthorized state depending on the result of the authentication exchange between the authentication server and the supplicant. Default is Auto.

reAuthMax: The number of authentication attempts that are permitted before the port becomes unauthorized. Default is 2.

txPeriod: Time period to transmitted EAPOL PDU between the authenticator and the supplicant. Default is 30.

Quiet Period: Period of time during which the switch will not attempt to access the supplicant. Default is 60 seconds.

reAuthEnabled: Choose whether regular authentication will take place on this port. Default is on.

reAuthPeriod: Period of time between the periodic re-authentication of the supplicant. Default is 3600.

max. Request: The maximum number of times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. Valid from 1-10. Default is 2.

times suppTimeout: Timeout condition in the exchange between the authenticator and the supplicant. Valid from 1-65535. Default is 30 seconds.

serverTimeout: Timeout condition in the exchange between the authenticator and the authentication server. Valid from 1-65535. Default is 30 seconds.

3.16 Alarm Configuration

3.16.1 Events

The Trap Events Configuration page (Figure 3-52) allows the user to select which events will be sent to the network administrator using which alert type. The switch supports 24 different trap events. The trap information can be sent out in three ways, email, mobile phone SMS (short message system) and SNMP traps. To enable a trap to be sent using a specific method, check the box beside the event and under the desired notification method.

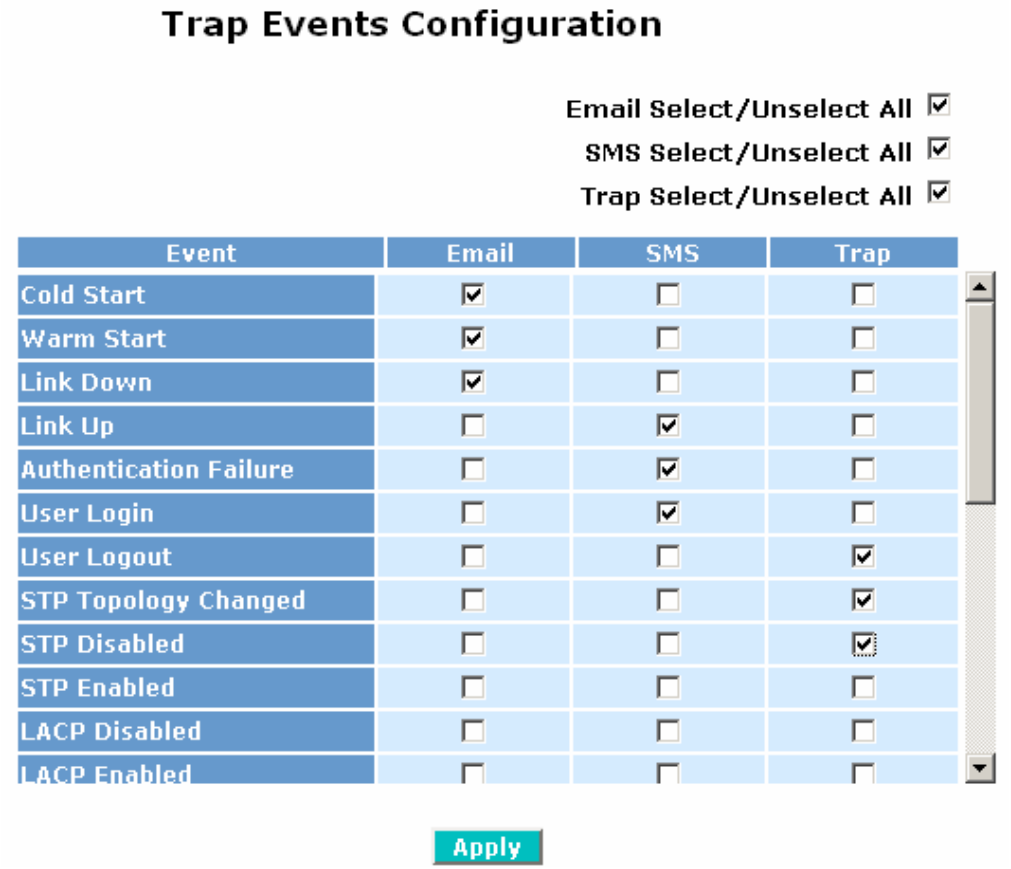

Figure 3-52: Trap Events Configuration Page

Trap types:

System traps: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout

STP: STP Topology Changed, STP Disabled, STP Enabled

LACP: LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure

GVRP: GVRP Disabled, GVRP Enabled

VLAN: VLAN Disabled, Port-based VLAN Enabled, Tag-based VLAN Enabled, Metro-mode VLAN Enabled, Double-tag VLAN Enabled

Module Swap: Module Inserted, Module Removed, Dual Media Swapped

3.16.2 Email/SMS

The Email/SMS Configuration page (figure 3-53) allows the user to configure the email and SMS settings for the switch to use to contact the network administrator. An email address and/or a mobile phone number has to be set in order for traps to be sent to users using those methods. The switch supports up to 6 email addresses and 6 mobile phone numbers. The 24 different trap events will also be sent to an SNMP Manager when a trap event occurs. Click “Apply” to save the changes once entered.

Note: SMS may not work with your mobile phone carrier. Different carriers use different customizations. This should be tested before being used in a live environment.

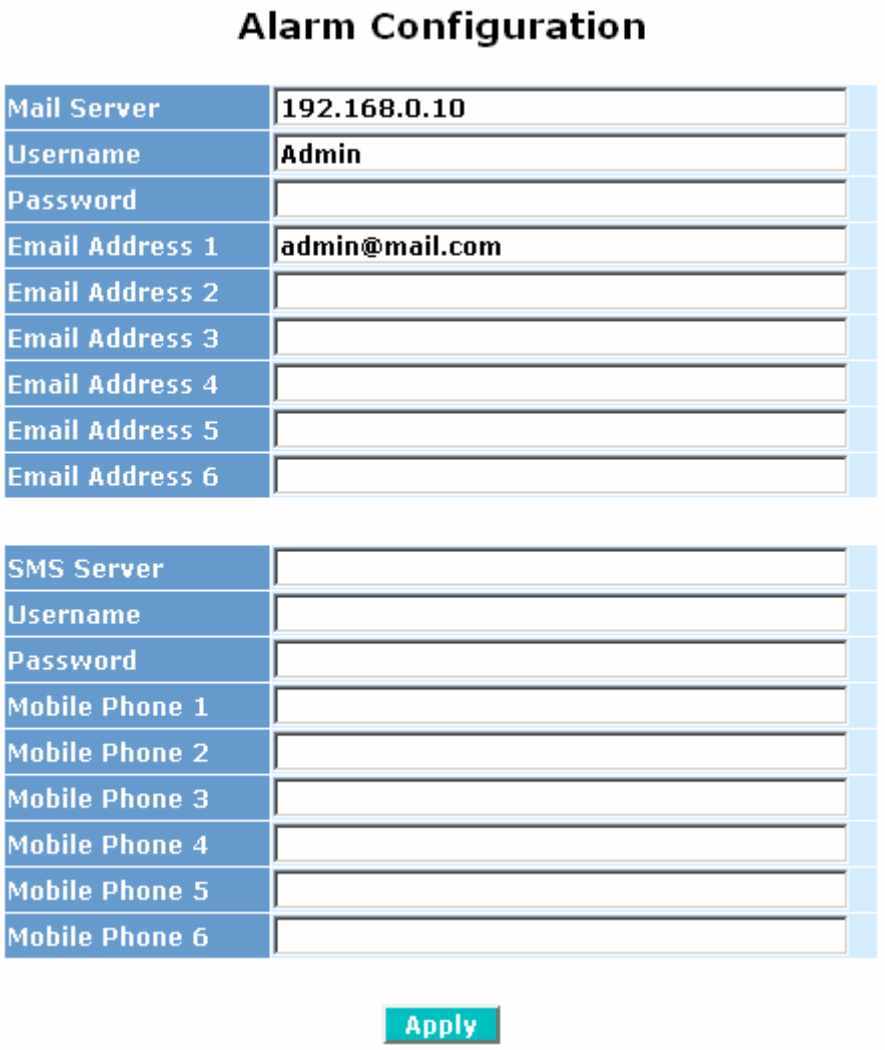

Figure 3-53: Alarm Configuration Page

Mail Server: The IP address of the SMTP server.

Username: The username on the SMTP server used for authentication.

Password: The password on the SMTP server used for authentication.

Email Address 1-6: The email addresses to send the alarm messages to.

SMS Server: The IP address of the SMS server (contact your cell carrier to find out if this is supported).

Username: The username for your ISP.

Password: The password for your ISP.

Mobile Phone 1-6: The mobile phone numbers to send the alarm messages to.

3.17 Configuration

The switch saves up to three version of the configuration file. The first is the factory default settings, the switch can be restored to these settings should any problems arise during configuration. The second is the startup or working configuration, this is the configuration that the switch uses when it starts up, and this is updated every time you click “Apply” in the GUI. The last is the user configuration, which is a user-defined backup configuration which can also be restored as the working configuration if desired.

3.17.1 Save/Restore

The Save/Restore page (Figure 3-54) allows users to save or restore their configuration settings.

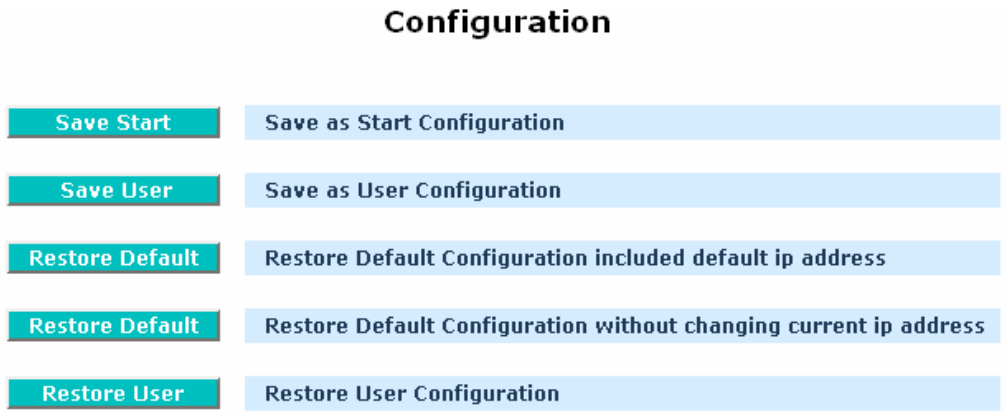

Figure 3-54: Configuration Page

Save Start: Saves the current configuration as the startup or working configuration in flash memory.

Save User: Saves the current configuration as the backup user configuration in flash memory.

Restore Default (including IP address): Restores the switch’s working configuration to factory defaults, including changing the IP address of the switch back to 192.168.1.1.

Restore Default (not including IP address): Restores the switch’s working configuration back to factory defaults, without changing the IP address.

Restore User Configuration: Restores the saved user configuration as the working configuration. Once completed, the system must be restarted for the new settings to take effect.

3.17.2 Config File

The Config File page (Figure 3-55) allows the user to save the current configuration to a file on the local computer, and to restore the configuration of the switch from a file saved on the local computer, using TFTP. See section 3.19 for details on changing the TFTP server settings.

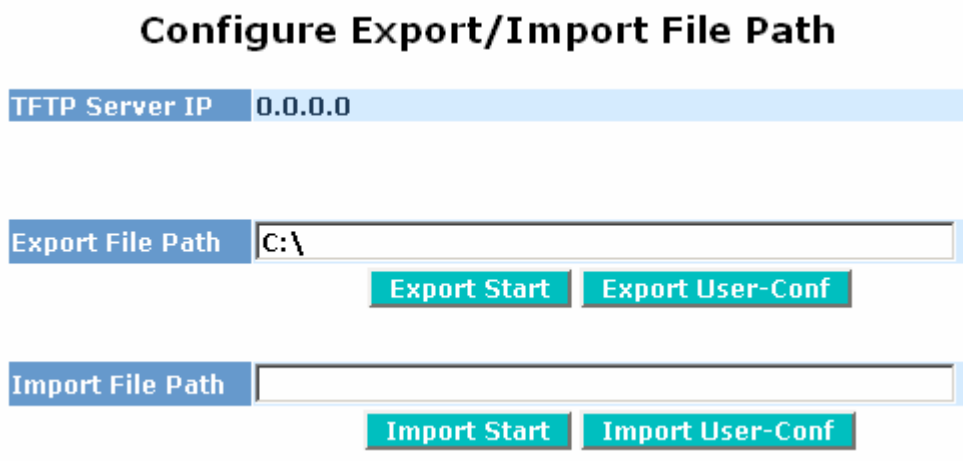

Figure 3-55: Configure File Path Page

Export File Path: The name and path to use when saving the file.

Export Start: Export the switch's startup configuration stored in flash to the local computer.

Export User-Conf: Export the switch's user configuration stored in flash to the local computer.

Import File Path: The name and path to use when retrieving the file.

Import Start: Overwrite the switch's startup configuration stored in flash with the file from the local computer.

Import User-Conf: Overwrite the switch's user configuration stored in flash with the file from the local computer.

3.18 Diagnostics

Three functions including Diagnostics, Loopback Test and Ping Test are contained in this section for self-diagnostics. Each of them will be described in the following sections.

3.18.1 Diagnostics

The Diagnostics page (Figure 3-56) provides a set of basic system diagnoses. It lets the user know whether the system is healthy or needs to be repaired. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.

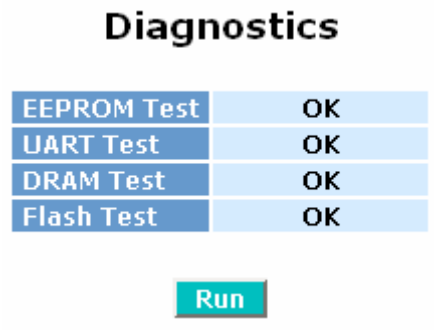

Figure 3-56: Diagnostics Page

3.18.2 Loopback

The Loopback Test page (Figure 3-59) provides two different loopback tests. One is an Internal Loopback Test and the other is an External Loopback Test. The former test will not send test signals outside the switch. The test signal only tests the signals within the switch. The latter test sends the test signal to the device connected to the other end. If the cable is not connected to an active network device, the switch will report that the external loopback test has failed.

> **Note:** Whatever you choose Internal Loopback Test or External Loopback Test, these two functions will interfere with normal system operations, and all packets will stop being sent and received temporarily.

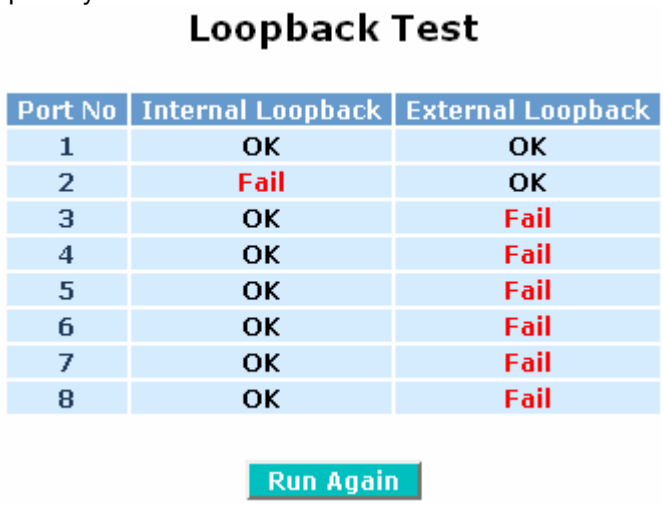

Figure 3-57: Loopback Test Page

3.18.3 Ping Test

The Ping Test page (Figure 3-58) allows the user to perform a ping on an external address to see if the remote device is accessible or not via ICMP protocol. To perform a test, enter the IP address to ping and click “Ping”. The results of the ping will appear after a few seconds.

> **Note:** Some devices may not reply to a ping even though they are active and working properly, depending on how they are configured. Many software firewalls on computers will prevent the computer from replying to a ping request.

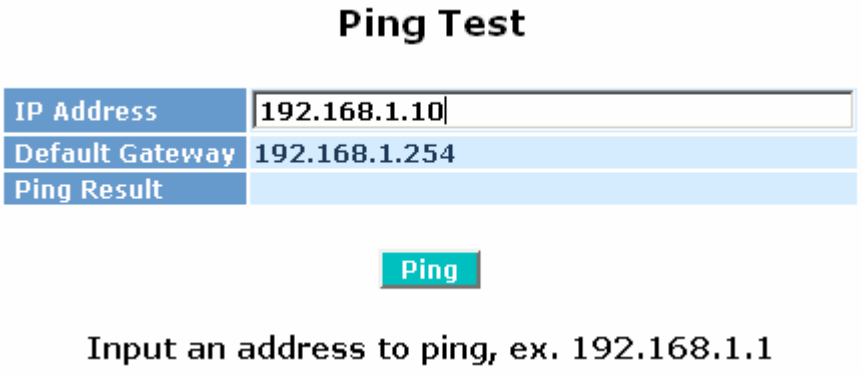

Figure 3-58: Ping Test Page

3.19 TFTP Server

The TFTP Server page (Figure 3-59) allows the user to set the TFTP server for the switch to use to send and receive files from a local computer on the network. Enter the IP address of the server and click “Apply” to save the changes.

Figure 3-59: TFTP Server Page

3.20 Log

The Log page (Figure 3-60) shows the log of system events. There are 19 private trap logs and 5 public trap logs that are stored in the log which correspond to the SNMP trap events. The switch supports a total of 120 log entries. For more details on log entries, refer to the section on Trap/Alarm Configuration and SNMP Configuration. In the report table, No., Time and Events are displayed for each trap record.

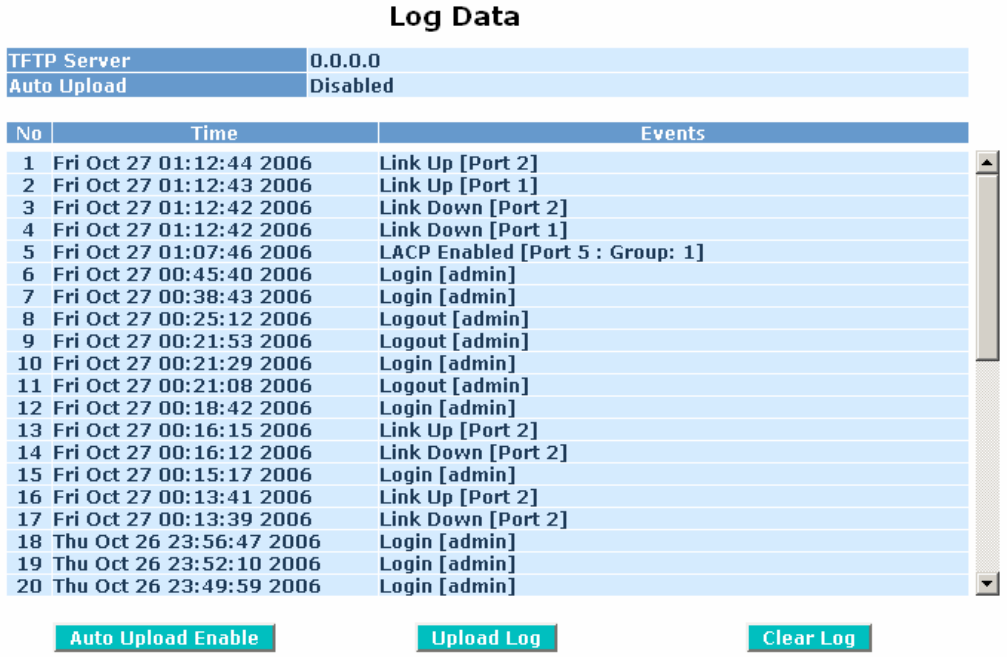
Log Data
TFTP Server 0.0.0.0
Auto Upload Disabled
No Time Events
1 Fri Oct 27 01:12:44 2006 Link Up [Port 2]
2 Fri Oct 27 01:12:43 2006 Link Up [Port 1]
3 Fri Oct 27 01:12:42 2006 Link Down [Port 2]
4 Fri Oct 27 01:12:42 2006 Link Down [Port 1]
5 Fri Oct 27 01:07:46 2006 LACP Enabled [Port 5 : Group: 1]
6 Fri Oct 27 00:45:40 2006 Login [admin]
7 Fri Oct 27 00:38:43 2006 Login [admin]
8 Fri Oct 27 00:25:12 2006 Logout [admin]
9 Fri Oct 27 00:21:53 2006 Logout [admin]
10 Fri Oct 27 00:21:29 2006 Login [admin]
11 Fri Oct 27 00:21:08 2006 Logout [admin]
12 Fri Oct 27 00:18:42 2006 Login [admin]
13 Fri Oct 27 00:16:15 2006 Link Up [Port 2]
14 Fri Oct 27 00:16:12 2006 Link Down [Port 2]
15 Fri Oct 27 00:15:17 2006 Login [admin]
16 Fri Oct 27 00:13:41 2006 Link Up [Port 2]
17 Fri Oct 27 00:13:39 2006 Link Down [Port 2]
18 Thu Oct 26 23:56:47 2006 Login [admin]
19 Thu Oct 26 23:52:10 2006 Login [admin]
20 Thu Oct 26 23:49:59 2006 Login [admin]
Auto Upload Enable
Upload Log
Clear Log

Figure 3-60: Log Data Table

No.: Display the order in which the trap occured.

Time: Display the time that the trap occured.

Events: Display the trap event name.

Auto Upload Enable: Switch the enabled or disabled status of the auto upload function, which will upload the log through TFTP automatically.

Upload Log: Upload log data through TFTP.

Clear Log: Clear log data.

3.21 Firmware Upgrade

The Firmware Upgrade page (Figure 3-61) allows you to update the firmware on the switch with new firmware that is provided by the manufacturer. Software upgrades typically improve the performance or increase the feature set of the switch. The switch requires a TFTP client running on a computer on the network for firmware upgrades.

To upgrade the firmware, first enter the IP address of the computer with the TFTP client and the new firmware on it under TFTP server (see section 3.19), then specify the filename of the firmware on the computer. Click “Upgrade” to complete the procedure. Once the upload has finished, the switch will start upgrading software. A reboot message will be displayed after the software has been upgraded. At this time, you must reboot the switch for the new software to take effect.

Warning: Powering off the switch in the middle of a firmware upgrade may cause the memory in the switch to be corrupted and cause the switch to stop working completely.

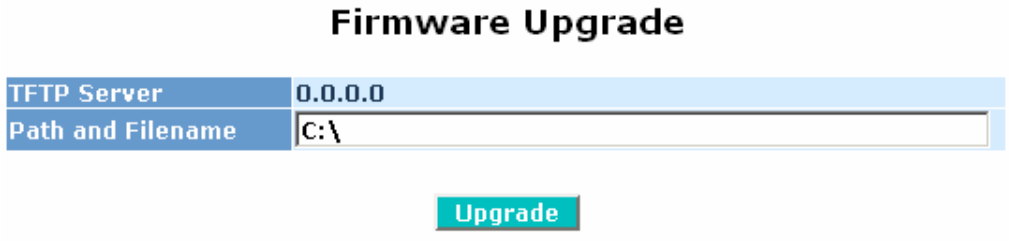

Figure 3-61: Firmware Upgrade Page

3.22 Reboot

The Reboot page (Figure 3-62) allows the user to reboot the switch through the web interface. Rebooting using this page is the same as pressing the reset button on the switch. It takes approximately 30 seconds for the switch to boot up.

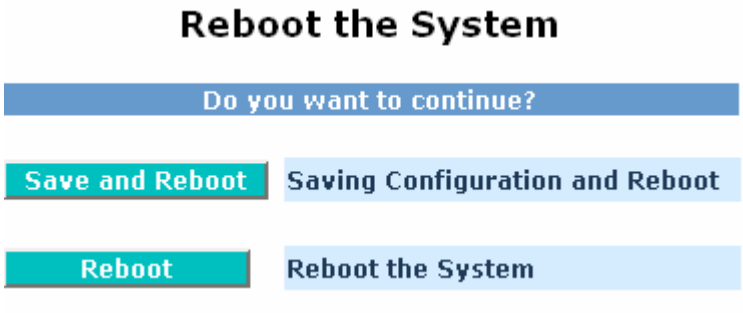

Figure 3-62: Reboot Page

Save and Reboot: Save the current settings as the start configuration before rebooting the switch.

Reboot: Reboot the switch without saving the current settings.

3.23 Logout

The Logout page (Figure 3-63) allows the user to log out of the web interface.

Figure 3-63: Logout Page

4 CLI Interface

4.1 CLI Management

The command-line interface (CLI) is a text-based interface into the switch. To use the CLI, you can Telnet into the switch, or you can connect to the switch's RS-232 port. The following are detailed instructions to set up an RS-232 connection:

1. Take the null modem cable that comes with the switch out of the box.
2. Connect one end of the cable into the RS-232 serial port on the switch, and the other end into an RS-232 serial port on your computer.
3. Start a terminal program on your computer (by default Windows uses HyperTerminal)
4. Configure the connection as shown below.

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	none

To Telnet into the switch, connect to the Ethernet port of the switch, and then open a command prompt in Windows. In the command prompt, type "telnet <ip address>" where <ip address> is the IP address of the switch. The same rules apply to connecting to the switch via Telnet as via the web interface in terms of being on the same subnet as the switch.

4.1.1 Login

The default username and password are shown below. Be sure to change the password as soon as possible for security purposes.

Username: admin

Password: admin

After you login successfully, you will see a prompt "SS2GD8I#" if you are the first person to login and you have administrator rights, otherwise the prompt may appear as "SS2GD8I$". The former means you have administrator rights and have full access to the switch. The latter means you only have guest rights and are only allowed to view the system without changing any settings.

4.2 CLI Commands

To see the commands available, use the "?" command at the prompt. Commands fall into two categories, global commands and local commands. Global commands can be used at any time and are listed in section 4.2.1, whereas local commands only work in a specific submenu and are listed in section 4.2.2. The same local command will perform different functions depending on which submenu the user is currently in.

4.2.1 CLI Global Commands

end

Syntax: end

Description: Returns you to the root menu. When you enter this command, you will be returned to the root menu regardless of which submenu you are in. If you use this command while in the root menu, you will remain in the root menu.

Arguments: None.

Example:

```
SS2GD8I# alarm
SS2GD8I(alarm)# events
SS2GD8I(alarm-events)# end
SS2GD8I#
```

exit

Syntax: exit

Description: Brings you up one menu level. When you enter this command, you will be move up to the parent menu. If you use this command while in the root menu, you will remain in the root menu.

Arguments: None.

Example:

```
SS2GD8I# alarm
SS2GD8I(alarm)# events
SS2GD8I(alarm-events)# exit
SS2GD8I(alarm)#
```

help

Syntax: help

Description: Shows a list of available commands. Some commands are a combination of two or more words.

Arguments: None.

Example:

```
SS2GD8I# ip
SS2GD8I(ip)# help
Commands available:
------------<< Local commands >>------------
set ip              Set ip,subnet mask and gateway
set dns             Set dns
enable dhcp         Enable DHCP, and set dns auto or manual
disable dhcp        Disable DHCP
show                Show IP Configuration
------------<< Global commands >>------------
exit                Back to the previous mode
end                 Back to the top mode
help                Show available commands
history             Show a list of previously run commands
logout              Logout the system
save start          Save as start config
save user           Save as user config
restore default     Restore default config
restore user        Restore user config
```

history

Syntax: history [#]

Description: Displays a list of previous commands that have been entered during this session. When you enter this command, a list of commands which have been entered before is displayed. The CLI supports up to 256 records. If no argument is used, the entire list is displayed, up to 256. If an optional argument is given, only the specified number of records will be shown.

Arguments: [#] (optional): the number of history records to show, range from 1-256.

Example 1:

```
SS2GD8I(ip)# history
Command history:
0. trunk
1. exit
2. SS2GD8I# trunk
3. SS2GD8I(trunk)# exit
4. SS2GD8I#
5. ?
6. trunk
7. exit
8. alarm
9. events
10. end
11. ip
12. help
13. ip
14. history
```

Example 2:

```
SS2GD8I(ip)# history 3
Command history:
13. ip
14. history
15. history 3
SS2GD8I(ip)#
```

logout

Syntax: logout

Description: When you enter this command, you will be logged out of the system and disconnected. If you are connected the switch through the serial port, you will be logged out of the system and be brought back to the initial login prompt.

Arguments: None.

Example:

```
SS2GD8I# logout
```

restore default

Syntax: restore default

Description: When you enter this command, you will receive a prompt saying “Do you want to restore the default IP address? (y/n)”. If you choose Y or y, the IP address will be restored to the default “192.168.1.1”. If you choose N or n, the IP address will not be changed.

If the unit was successfully restored to defaults, you will see a prompt asking if you want to reboot immediately or not. If you press Y or y, the system will reboot immediately; otherwise, you will be taken back to the CLI prompt. After restoring to defaults, all of the changes in the system will be erased, and the unit will be reset to factory defaults after being rebooted.

Arguments: None.

Example:

```
SS2GD8I# restore default
Restoring ...
Restore Default Configuration Successfully
Press any key to reboot system.
```

restore user

Syntax: restore user

Description: Restores the startup configuration with the saved user configuration. After restoring the user-defined configuration, all the changes in the startup configuration will be lost. After rebooting, the startup configuration will be replace with the user defined one. This function requires that a user configuration be saved first using the “save user” command.

Arguments: None.

Example:

```
SS2GD8I# restore user
Restoring ...
Restore User Configuration Successfully
Press any key to reboot system.
```

save start

Syntax: save start

Description: Saves the current configuration as the startup configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. You must enter this command after making any changes in the CLI in order for the changes to remain after the unit is restarted.

Arguments: None.

Example:

```
SS2GD8I# save start
Saving start...
Save Successfully
SS2GD8I#
```

save user

Syntax: save user

Description: Saves the current configuration as the user-defined configuration. This is a backup configuration that can be loaded in the future, but is not currently active.

Arguments: None.

Example:

```
SS2GD8I# save user
Saving user...
Save Successfully
SS2GD8I#
```

4.2.2 Local Commands of CLI

> 802.1X

set max-request

Syntax: set max-request <port-range> <times>

Description: The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before the authentication session times out.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<times>: maximum number of tries, range from 1-10, default is 2.

Example:

```
SS2GD8I(802.1X)# set max-request 2 2
```

set mode

Syntax: set mode <port-range> <mode>

Description: Sets the 802.1X authentication mode for each port.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<mode>: 0 or 1 (off or on).

Example:

```
SS2GD8I(802.1X)# set mode 2 1
```

set port-control

Syntax: set port-control <port-range> <authorized>

Description: Set the 802.1X status of each port.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<authorized>: Port status (0, 1, or 2).

0: ForceUnauthorized

1: ForceAuthorized

2: Auto

Example:

```
SS2GD8I(802.1X)# set port-control 2 2
```

set quiet-period

Syntax: set quiet-period <port-range> <sec>

Description: A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<sec>: timer, range from 0-65535, default is 60.

Example:

```
SS2GD8I(802.1X)# set quiet-period 2 30
```

set reAuthEnabled

Syntax: set reAuthEnabled <port-range> <ebl>

Description: A constant that defines whether regular reauthentication will take place on this port or not.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<ebl>: 0 or 1 (disable or enable re-authentication).

Example:

```
SS2GD8I(802.1X)# set reAuthEnabled 2 1
```

set reAuthMax

Syntax: set reAuthMax <port-range> <max>

Description: The number of re-authentication attempts that are permitted before the port becomes Unauthorized.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<max>: number of attempts, range from 1-10, default is 2.

Example:

```
SS2GD8I(802.1X)# set reAuthMax 2 2
```

set reAuthPeriod

Syntax: set reAuthPeriod <port-range> <sec>

Description: The number of seconds between re-authenticating the supplicant.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<sec>: timer, range from 1-65535, default is 3600.

Example:

```
SS2GD8I(802.1X)# set reAuthPeriod 2 3600
```

set serverTimeout

Syntax: set serverTimeout <port-range> <sec>

Description: Sets the timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<sec>: timer, range from 1-65535, default is 30

Example:

```
SS2GD8I(802.1X)# set serverTimeout 2 30
```

set state

Syntax: set state <ip> <port-number> <secret-key>

Description: Configures the settings of the 802.1X Radius Server.

Arguments:

<ip>: the IP address of Radius Server

<port-number>: the service port (authorization port) of the Radius Server, from 1-65535, default is 1812

<secret-key>: the value of the secret-key which has to have a length between 1 and 31 characters

Example:

```
SS2GD8I(802.1X)# set state 192.168.1.115 1812 WinRadius
```

set suppTimeout

Syntax: set suppTimeout <port-range> <sec>

Description: Sets the timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<sec>: timer , range from 1-65535, default is 30.

Example:

```
SS2GD8I(802.1X)# set suppTimeout 2 30
```

set txPeriod

Syntax: set txPeriod <port-range> <sec>

Description: Sets the timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted

Arguments:

<port range>: which ports are affected, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<sec>: timer, range from 1-65535, default is 30.

Example:

```
SS2GD8I(802.1X)# set txPeriod 2 30
```

show mode

Syntax: show mode

Description: Displays the mode of each port.

Arguments: None.

Example:

```
SS2GD8I(802.1X)# show mode
Port     Mode
====== ============
1       Disable
2       Multi-host
3       Disable
4       Disable
5       Disable
6       Disable
```

show parameter

Syntax: show parameter

Description: Displays the parameter settings of each port.

Arguments: None

Example:

```
SS2GD8I(802.1X)# show parameter
port 1)  port control    : Auto
         reAuthMax       : 2
         txPeriod        : 30
         Quiet Period    : 60
         reAuthEnabled   : ON
         reAuthPeriod    : 3600
         max. Request    : 2
         suppTimeout     : 30
         serverTimeout   : 30
port 2)  port control    : Auto
         reAuthMax       : 2
         txPeriod        : 30
         Quiet Period    : 60
         reAuthEnabled   : ON
         reAuthPeriod    : 3600
         max. Request    : 2
         suppTimeout     : 30
         serverTimeout   : 30
```

show security

Syntax: show security

Description: Displays the authentication status of each port.

Arguments: None

Example:

```
SS2GD8I(802.1X)# show security
Port    Mode         Status
====== ============ ==============
1       Disable
2       Multi-host   Unauthorized
3       Disable
4       Disable
5       Disable
6       Disable
```

show state

Syntax: show state

Description: Shows the Radius server configuration

Arguments: None

Example:

```
SS2GD8I(802.1X)# show state
Radius Server  : 192.168.1.115
Port Number    : 1812
Secret Key     : WinRadius
```

> account

add

Syntax: add <name>

Description: Creates a new guest user. When you create a new guest user, you must type in a password and confirm the password.

Arguments:

<name>: new account name, must be at least 5 characters long.

Example:

```
SS2GD8I(account)# add aaaaa
Password:
Confirm Password:
Save Successfully
SS2GD8I(account)#
```

del

Syntax: del <name>

Description: Deletes an existing user account.

Arguments: <name>: existing user account name.

Example:

```
SS2GD8I(account)# del aaaaa
Account aaaaa deleted
```

modify

Syntax: modify <name>

Description: Changes the username and password of an existing account.

Arguments:

<name>: existing user account name.

Example:

```
SS2GD8I(account)# modify aaaaa
username/password: the length is from 5 to 15.
Current username (aaaaa):bbbbb
New password:
Confirm password:
Username changed successfully.
Password changed successfully.
```

show

Syntax: show

Description: Shows system accounts, including account name and identity.

Arguments: None.

Example:

```
SS2GD8I(account)# show
Account Name   Identity
-------------- ---------------
admin          Administrator
guest          guest
```

> alarm

>> email

del mail-address

Syntax: del mail-address <#>

Description: Removes the configuration of an e-mail address.

Arguments:

<#>: email address number, range from 1 to 6.

Example:

```
SS2GD8I(alarm-email)# del mail-address 2
```

del server-user

Syntax: del server-user

Description: Removes the configuration of an email server including user account and password.

Arguments: None.

Example:

```
SS2GD8I(alarm-email)# del server-user
```

set mail-address

Syntax: set mail-address <#> <mail address>

Description: Sets up an email address.

Arguments:

<#>: email address number, range from 1 to 6.

<mail address>: email address

Example:

```
SS2GD8I(alarm-email)# set mail-address 1 abc@mail.abc.com
```

set server

Syntax: set server <ip>

Description: Sets the IP address of the email server.

Arguments:

<ip>: email server IP address or domain name

Example:

```
SS2GD8I(alarm-email)# set server 192.168.1.6
```

set user

Syntax: set user <username>

Description: Sets the account and password of the email server. After you enter the user name, you will be prompted for the password.

Arguments:

<username>: email server account and password

Example:

```
SS2GD8I(alarm-email)# set user admin
```

show

Syntax: show

Description: Displays the e-mail alerts configuration.

Arguments: None.

Example:

```
SS2GD8I(alarm-email)# show
Mail Server    : 192.168.1.6
Username : admin
Password : ****************
Email Address 1: abc@mail.abc.com
Email Address 2:
Email Address 3:
Email Address 4:
Email Address 5:
Email Address 6:
```

>> events

del all

Syntax: del all <range>

Description: Disables events from being sent out via email, sms and traps.

Arguments:

<range>: which events to delete, can be a single event (e.g. “1”) or a range of events (e.g. “5-7”), range from 1-24.

Example:

```
SS2GD8I(alarm-events)# del all 1-3
```

del email

Syntax: del email <range>

Description: Disables events from being sent out via email.

Arguments:

<range>: which events to delete, can be a single event (e.g. “1”) or a range of events (e.g. “5-7”), range from 1-24.

Example:

```
SS2GD8I(alarm-events)# del email 1-3
```

del sms

Syntax: del sms <range>

Description: Disables events from being sent out via SMS.

Arguments:

<range>: which events to delete, can be a single event (e.g. “1”) or a range of events (e.g. “5-7”), range from 1-24.

Example:

```
SS2GD8I(alarm-events)# del sms 1-3
```

del trap

Syntax: del trap <range>

Description: Disables events from being sent out via traps.

Arguments:

<range>: which events to delete, can be a single event (e.g. “1”) or a range of events (e.g. “5-7”), range from 1-24.

Example:

```
SS2GD8I(alarm-events)# del trap 1-3
```

set all

Syntax: set all <range>

Description: Enables events to be sent out via email, SMS and traps.

Arguments:

<range>: which events to delete, can be a single event (e.g. “1”) or a range of events (e.g. “5-7”), range from 1-24.

Example:

```
SS2GD8I(alarm-events)# set all 1-3
```

set email

Syntax: set email <range>

Description: Enables events to be sent out via email.

Arguments:

<range>: which events to delete, can be a single event (e.g. “1”) or a range of events (e.g. “5-7”), range from 1-24.

Example:

```
SS2GD8I(alarm-events)# set email 1-3
```

set sms

Syntax: set sms <range>

Description: Enables events to be sent out via SMS.

Arguments:

<range>: which events to delete, can be a single event (e.g. “1”) or a range of events (e.g. “5-7”), range from 1-24.

Example:

```
SS2GD8I(alarm-events)# set sms 1-3
```

set trap

Syntax: set trap <range>

Description: Enables events to be sent out via traps.

Arguments:

<range>: which events to delete, can be a single event (e.g. “1”) or a range of events (e.g. “5-7”), range from 1-24.

Example:

```
SS2GD8I(alarm-events)# set trap 1-3
```

show

Syntax: show

Description: Displays the configuration of alarm events.

Arguments: None.

Example:

```
SS2GD8I(alarm-events)# show
Events                      Email SMS Trap
-----------------------------------------
1  Cold Start                         v
2  Warm Start                         v
3  Link Down                          v
4  Link Up                            v
5  Authentication Failure             v
6  User Login
7  User Logout
8  STP Topology Changed
9  STP Disabled
10 STP Enabled
11 LACP Disabled
12 LACP Enabled
13 LACP Member Added
14 LACP Port Failure
15 GVRP Disabled
16 GVRP Enabled
17 VLAN Disabled
18 Port-based Vlan Enabled
19 Tag-based Vlan Enabled
20 Metro-mode Vlan Enabled
21 Double-tag Vlan Enabled
22 Module Inserted
23 Module Removed
24 Module Media Swapped
```

show (alarm)

Syntax: show <alarm>

Description: Displays the configuration of a specific alarm type.

Arguments:

<alarm>: alarm type, can be “events”, “email”, or “sms”.

Example:

```
SS2GD8I(alarm)# show events
SS2GD8I(alarm)# show email
SS2GD8I(alarm)# show sms
```

>> sms

del phone-number

Syntax: del phone-number <#>

Description: Deletes an SMS phone number.

Arguments:

<#>: mobile phone number, range from 1 to 6

Example:

```
SS2GD8I(alarm-sms)# del phone-number 3
```

del server-user

Syntax: del server-user

Description: Removes the configuration of an SMS server including user account and password.

Arguments: None.

Example:

```
SS2GD8I(alarm-sms)# del server-user
```

set phone-number

Syntax: set phone-number <#> <phone-number>

Description: Adds an SMS phone number.

Arguments:

<#>: SMS slot number, range from 1 to 6

<phone-number>: phone number

Example:

```
SS2GD8I(alarm-sms)# set phone-number 1 8181234567
```

set server

Syntax: set server <ip>

Description: Sets the IP address of the SMS server.

Arguments:

<ip>: SMS server IP address or domain name

Example:

```
SS2GD8I(alarm-sms)# set server 192.168.1.7
```

set user

Syntax: set user <username>

Description: Sets the user account and password of the SMS server.

Arguments:

<username>: SMS server account

Example:

```
SS2GD8I(alarm-sms)# set user ABC
```

show

Syntax: show

Description: Display the configuration of the SMS trap event.

Arguments: None.

Example:

```
SS2GD8I(alarm-sms)# show
SMS Server        : 192.168.1.7
Username          : ABC
Password          : ****************
Mobile Phone 1    : 8181234567
Mobile Phone 2    :
Mobile Phone 3    :
Mobile Phone 4    :
Mobile Phone 5    :
Mobile Phone 6    :
```

> autologout

autologout

Syntax: autologout <time>

Description: Set the timer before the user is automatically logged out..

Arguments:

<time>: range from 1 to 3600 seconds, 0 to turn autologout off, default is 180.

Example:

```
SS2GD8I# autologout 3600
Set autologout time to 3600 seconds
```

> bandwidth

disable egress-rate

Syntax: disable egress-rate <port range>

Description: Cancel the egress-rate setting of a port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(bandwidth)# disable egress-rate 1-8
```

disable ingress-rate

Syntax: disable ingress-rate <port range>

Description: Cancels the ingress-rate setting of a port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(bandwidth)# disable ingress-rate 1-8
```

disable storm-rate

Syntax: disable storm-rate <port range>

Description: Cancels the storm-rate of a port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(bandwidth)# disable storm-rate 1-8
```

enable egress-rate

Syntax: enable egress-rate <port range> <data rate>

Description: Sets the egress-rate of a port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<data rate>: the egress-rate limit in Mbps, range from 0-1000

Example:

```
SS2GD8I(bandwidth)# enable egress-rate 1-8 200
```

enable ingress-rate

Syntax: enable ingress-rate <range> <data rate>

Description: Sets the ingress-rate of a port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<data rate>: the ingress-rate limit in Mbps, range from 0-1000

Example:

```
SS2GD8I(bandwidth)# enable ingress-rate 1-8 100
```

enable storm-rate

Syntax: enable storm-rate <range> <data rate>

Description: Sets the storm-rate of a port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<data rate>: the storm-rate limit in Mbps, range from 0-1000

Example:

```
SS2GD8I(bandwidth)# enable strom-rate 1-8 150
```

show

Syntax: show

Description: Displays all current bandwidth limitation settings.

Arguments: None.

Example:

```
SS2GD8I(bandwidth)# show
                    Ingress                         Egress
     ======================================== ==================
Port All State All Rate Storm State Storm Rate All state All Rate
==== ========= ======== =========== ========== ========= ========
  1   Disabled     0      Disabled        0      Disabled     0
  2   Disabled     0      Disabled        0      Disabled     0
  3   Disabled     0      Disabled        0      Disabled     0
  4   Disabled     0      Disabled        0      Disabled     0
  5   Disabled     0      Disabled        0      Disabled     0
  6   Disabled     0      Disabled        0      Disabled     0
  7   Disabled     0      Disabled        0      Disabled     0
  8   Disabled     0      Disabled        0      Disabled     0
```

> config-file

set export-path

Syntax: set export-path <file path>

Description: Sets the path and filename that settings will be exported to (relative to the root directory of the TFTP server).

Arguments:

<file path>: path and file name

Example:

```
SS2GD8I(config-file)# set export-path log/21511.txt
```

export start

Syntax: export start

Description: Exports startup settings to the file defined using *set export-path*.

Arguments: None.

Example:

```
SS2GD8I(config-file)# export start
Export successful.
```

export user-conf

Syntax: export user-conf

Description: Exports user configuration settings to the file defined using *set export-path*.

Arguments: None.

Example:

```
SS2GD8I(config-file)# export user-conf
Export successful.
```

set import-path

Syntax: set import-path <file path>

Description: Sets the path and filename that settings will be imported from (relative to the root directory of the TFTP server).

Arguments:

<file path>: path and filename

Example:

```
SS2GD8I(config-file)# set import-path log/21511.txt
```

import start

Syntax: import start

Description: Imports startup settings from the file defined using *set import-path*.

Arguments: None.

Example:

```
SS2GD8I(config-file)# import start
Import successful.
```

import user-conf

Syntax: import user-conf

Description: Imports user configuration settings from the file defined using *set import-path*.

Arguments: None.

Example:

```
SS2GD8I(config-file)# import user-conf
Import successful.
```

show

Syntax: show

Description: Displays the config-file import/export configuration.

Arguments: None.

Example:

```
SS2GD8I(config-file)# show
TFTP Server IP Address: 192.168.3.111
Export Path and Filename: nmap/123.ts
Import Path and Filename: user123.txt
```

> dhcp-boot

set dhcp-boot

Syntax: set dhcp-boot <sec>

Description: Sets the delay time for DHCP Boot.

Arguments:

<sec>: delay in seconds, range from 0-30, a value of 0 will disable dhcp-boot delay.

Example:

```
SS2GD8I(dhcp-boot)# set dhcp-boot 30
```

show

Syntax: show

Description: Displays the status of DHCP Boot.

Arguments: None.

Example:

```
SS2GD8I(dhcp-boot)# show
dhcp boot  : Enable
Second     : 10
```

> diag

diag

Syntax: diag

Description: Tests whether UART, DRAM, Flash and EEPROM are working normally or not.

Arguments: None.

Example:

```
SS2GD8I(diag)# diag
EEPROM Test    : OK
UART Test      : OK
DRAM Test      : OK
Flash Test     : OK
```

loopback

Syntax: loopback

Description: Tests internal/external loopback.

Arguments: None.

Example:

```
SS2GD8I(diag)# loopback
Internal Loopback Test : OK
External Loopback Test : Port 1 2 3 4 5 6 7 8 Fail
```

ping

Syntax: ping <ip>

Description: Tests if the switch is able to ping a specific IP address or domain.

Arguments:

<ip>: IP address or domain name (e.g. 192.168.0.100 or www.yahoo.com)

Example:

```
SS2GD8I(diag)# ping 192.168.1.115
Gateway  : 192.168.1.253
192.168.1.115 is alive.
```

> firmware

set upgrade-path

Syntax: set upgrade-path <file path>

Description: To set up the image file that will be upgraded.

Arguments:

<file path>: upgrade file path (relative to the root directory of the TFTP server).

Example:

```
SS2GD8I(firmware)# set upgrade-path gs2108c_SS2GD8I_v2.03.img
```

show

Syntax: show

Description: Displays information for the TFTP server and upgrade path.

Arguments: None.

Example:

```
SS2GD8I(firmware)# show
TFTP Server IP Address  : 192.168.3.111
Path and Filename       : gs2108c_SS2GD8I_v2.03.img
```

upgrade

Syntax: upgrade

Description: Upgrades the firmware using the path and file defined using *set upgrade-path*.

Arguments: None.

Example:

```
SS2GD8I(firmware)# upgrade
Upgrading firmware ...
```

> gvrp

disable

Syntax: disable

Description: Disables GVRP.

Arguments: None.

Example:

```
SS2GD8I(gvrp)# disable
```

enable

Syntax: enable

Description: Enables GVRP.

Arguments: None.

Example:

```
SS2GD8I(gvrp)# enable
```

group

Syntax: group <group number>

Description: Selects which GVRP group is currently actively worked on. After a group is selected, the commands below can be used to modify the settings for this group.

Arguments:

<group number>: the VID of the GVRP group number to select, range from 1-4094

Example:

```
SS2GD8I(gvrp)# show group
GVRP group information
Current Dynamic Group Number: 1
VID      Member Port
---- -------------------------------------------------
2        5
SS2GD8I(gvrp)# group 2
SS2GD8I(gvrp-group-2)# set applicant 1-6 non-participant
SS2GD8I(gvrp-group-2)# show
GVRP group VID: 2
Port  Applicant       Registrar
----  --------------  ---------
1     Non-Participant  Normal
2     Non-Participant  Normal
3     Non-Participant  Normal
4     Non-Participant  Normal
5     Non-Participant  Normal
6     Non-Participant  Normal
7     Normal           Normal
8     Normal           Normal
SS2GD8I(gvrp-group-2)# set registrar 1-8 fixed
SS2GD8I(gvrp-group-2)# show
GVRP group VID: 2
Port  Applicant       Registrar
----  --------------  ---------
1     Non-Participant  Fixed
2     Non-Participant  Fixed
3     Non-Participant  Fixed
4     Non-Participant  Fixed
5     Non-Participant  Fixed
```

```
6      Non-Participant  Fixed
7      Normal           Fixed
8      Normal           Fixed
```

set applicant

Syntax: set applicant <port range> <type>

Description: Sets the default applicant mode for each port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<type>: applicant type, can be “normal” or “non-participant”

Example:

```
SS2GD8I(gvrp)# set applicant 1-8 non-participant
```

set registrar

Syntax: set registrar <port range> <type>

Description: Sets the default registrar mode for each port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<type>: registrar type, can be “normal”, “fixed”, or “forbidden”

Example:

```
SS2GD8I(gvrp)# set registrar 1-5 fixed
```

set restricted

Syntax: set restricted <port range> <status>

Description: Sets the restricted mode status for each port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<status> restricted mode status, either “enable” or “disable”

<enable|disable>: enable or disable

Example:

```
SS2GD8I(gvrp)# set restricted 1-8 enable
SS2GD8I(gvrp)# show config
GVRP state: Enable
Port Join Time Leave Time LeaveAll Time Applicant Registrar Restricted
---- --------- --------- -------------- --------- --------- ----------
  1     20         60          1000        Normal    Normal    Enable
  2     20         60          1000        Normal    Normal    Enable
  3     20         60          1000        Normal    Normal    Enable
  4     20         60          1000        Normal    Normal    Enable
  5     20         60          1000        Normal    Normal    Enable
  6     20         60          1000        Normal    Normal    Enable
  7     20         60          1000        Normal    Normal    Enable
  8     20         60          1000        Normal    Normal    Enable
```

set timer

Syntax: set timer <port range> <join> <leave> <leaveall>

Description: Sets GVRP join time, leave time, and leaveall time for each port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<join>: join timer, range from 20 to 100.

<leave>: leave timer, range from 60 to 300. Leave Time must equal to or greater than double the Join Time.

<leaveall>: leaveall timer, range from 1000 to 5000.

Example:

```
SS2GD8I(gvrp)# set timer 2-8 25 80 2000
```

show config

Syntax: show config

Description: Displays the GVRP configuration.

Arguments: None.

Example:

```
SS2GD8I(gvrp)# show config
GVRP state: Enable
Port Join Time Leave Time LeaveAll Time Applicant Registrar Restricted
---- --------- ---------- ------------- --------- --------- ----------
  1      20        60          1000        Normal    Normal    Disable
  2      25        80          2000        Normal    Normal    Disable
  3      25        80          2000        Normal    Normal    Disable
  4      25        80          2000        Normal    Normal    Disable
  5      25        80          2000        Normal    Normal    Disable
  6      25        80          2000        Normal    Normal    Disable
  7      25        80          2000        Normal    Normal    Disable
  8      25        80          2000        Normal    Normal    Disable
```

show counter

Syntax: show counter <port>

Description: Display the counter number of a port.

Arguments:

<port>: port number, range from 1 to 8.

Example:

```
SS2GD8I(gvrp)# show counter 2
GVRP Counter port: 2
Counter Name           Received  Transmitted
--------------------   --------  -----------
Total GVRP Packets     0         0
Invalid GVRP Packets   0         ----
LeaveAll message       0         0
JoinEmpty message      0         0
JoinIn message         0         0
LeaveEmpty message     0         0
Empty message          0         0
```

show group

Syntax: show group

Description: Show all GVRP groups.

Arguments: None.

Example:

```
SS2GD8I(gvrp)# show group
GVRP group information
VID      Member Port
---- ------------------------------------------------
```

> hostname

hostname

Syntax: hostname <name>

Description: Sets the hostname of the switch.

Arguments:

<name>: hostname, maximum 40 characters.

Example:

```
SS2GD8I# hostname Company
Company#
```

> igmp

set igmp_snooping

Syntax: set igmp_snooping <status>

Description: Set the mode for IGMP Snooping.

Arguments:

<status>: IGMP snooping status, can be one of the following: 0 for disabled, 1 for active, or 2 for passive.

Example:

```
SS2GD8I(igmp)# set igmp-snooping 2
```

show

Syntax: show

Description: Displays the IGMP snooping mode and IP Multicast Table.

Arguments: None.

Example:

```
SS2GD8I(igmp)# show
Snoop Mode: Active
IP Multicast:
1) IP Address  : 224.1.1.1
   VLAN ID     : 0
   Member Port : 22
```

> IP

disable dhcp

Syntax: disable dhcp

Description: Disables the DHCP server.

Arguments: None.

Example:

```
SS2GD8I(ip)# disable dhcp
```

enable dhcp

Syntax: enable dhcp <dns>

Description: Enables the DHCP server and set the DNS server to manual or auto mode.

Arguments:

<dns>: set DHCP by using manual or auto mode, can be “manual” or “auto”.

Example:

```
SS2GD8I(ip)# enable dhcp manual
```

set dns

Syntax: set dns <ip>

Description: Sets the IP address of DNS server.

Arguments:

<ip>: IP address of DNS server.

Example:

```
SS2GD8I (ip)# set dns 168.95.1.1
```

set ip

Syntax: set ip <ip> <mask> <gateway>

Description: Sets the system IP address, subnet mask and gateway.

Arguments:

<ip>: IP address.

<mask>: subnet mask.

<gateway>: default gateway.

Example:

```
SS2GD8I(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253
```

show

Syntax: show

Description: Displays the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.

Arguments: None.

Example:

```
SS2GD8I(ip)# show
DHCP                : Disable
IP Address          : 192.168.2.237
Current IP Address  : 192.168.2.237
Subnet mask         : 255.255.255.0
Gateway             : 192.168.2.252
DNS Setting         : Manual
DNS Server          : 168.95.1.1
```

> log

clear

Syntax: clear

Description: Clears the log data.

Arguments: None.

Example:

```
SS2GD8I(log)# clear
```

disable auto-upload

Syntax: disable auto-upload

Description: Disables auto-upload of the log.

Arguments: None.

Example:

```
SS2GD8I(log)# disable auto-upload
```

enable auto-upload

Syntax: enable auto-upload

Description: Enables auto-upload of the log.

Arguments: None.

Example:

```
SS2GD8I(log)# enable auto-upload
```

show

Syntax: show

Description: Shows a list of trap log events. Up to 120 log records are saved by the switch.

Arguments: None.

Example:

```
SS2GD8I(log)# show
Tftp Server : 0.0.0.0
Auto Upload : Disable
1)  Sat Jan 1 12:13:27 2005   Link Up [Port 1]
2)  Sat Jan 1 12:13:26 2005   Link Down [Port 1]
3)  Sat Jan 1 11:58:31 2005   Login [admin]
4)  Sat Jan 1 11:19:45 2005   Login [admin]
5)  Sat Jan 1 11:19:37 2005   Logout [admin]
```

upload

Syntax: upload

Description: Uploads log data through TFTP.

Arguments: None.

Example:

```
SS2GD8I(log)# upload
```

> mac-table

>> alias

del

Syntax: del <mac>

Description: Deletes the MAC address alias entry.

Arguments:

<mac>: MAC address, format: 00-02-03-04-05-06.

Example:

```
SS2GD8I(mac-table-alias)# del 00-44-33-44-55-44
```

set

Syntax: set <mac> <alias>

Description: Set the MAC address alias entry.

Arguments:

<mac>: MAC address, format: 00-02-03-04-05-06.

<alias>: MAC address alias name, maximum 15 characters.

Example:

```
SS2GD8I(mac-table-alias)# set 00-44-33-44-55-44 www
```

show

Syntax: show

Description: Displays the MAC address alias list.

Arguments: None.

Example:

```
SS2GD8I(mac-table-alias)# show
MAC Alias List
     MAC Address        Alias
---  -----------------  ---------------
1)   00-02-03-04-05-06  aaa
2)   00-33-03-04-05-06  ccc
3)   00-44-33-44-55-44  www
```

>> information

search

Syntax: search <port range> <mac> <vid>

Description: Looks for a specific MAC address in the MAC table.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<mac>: MAC address, format: 01-02-03-04-05-06, '?' can be used as a wildcard

<vid>: VLAN ID, range from 1 to 4094; '?' as a wildcard, or 0 as untagged

Example:

```
SS2GD8I(mac-table-information)# search 1-8 ??-??-??-??-??-?? ?
MAC Table List
Alias              MAC Address       Port  VID   State
---------------- ------------------ ---- ---- -----------------
                   00-40-c7-88-00-06   1     0   Dynamic
```

show

Syntax: show

Description: Displays the entire MAC address table.

Arguments: None.

Example:

```
SS2GD8I (mac-table-information)# show
MAC Table List
Alias              MAC Address       Port  VID   State
---------------- ------------------ ---- ---- -----------------
                   00-10-db-1d-c5-a0   8     0    Dynamic
                   00-40-f4-89-c9-7f   8     0    Dynamic
                   00-e0-18-2b-9d-e2   8     0    Dynamic
                   00-40-c7-d8-00-02   8     0    Dynamic
```

>> maintain

set aging

Syntax: set aging <#>

Description: Sets the aging time of MAC addresses that are learned dynamically.

Arguments:

<#>: age-timer in seconds, range from 10 to 65535, or 0 to disable aging

Example:

```
SS2GD8I(mac-table-maintain)# set aging 300
```

set flush

Syntax: set flush

Description: Deletes all MAC addresses that are learned dynamically.

Arguments: None.

Example:

```
SS2GD8I(mac-table-maintain)# set flush
```

show

Syntax: show

Description: Displays the settings of the age-timer.

Example:

```
SS2GD8I(mac-table-maintain)# show
age-timer : 300 seconds
```

>> static-mac

add

Syntax: add <mac> <port> <vid> [alias]

Description: Adds a static MAC entry.

Arguments:

<mac>: MAC address, format: 00-02-03-04-05-06

<port>: Port to assign MAC address to, range from 0-8. 0 means that this entry is for filtering only.

<vid>: VLAN ID, range from 0-4094. VID must be 0 if VLAN mode is not tag-based.

[alias] (optional): MAC alias name, maximum 15 characters

Example:

```
SS2GD8I(mac-table-static-mac)# add 00-02-03-04-05-06 3 0 aaa
```

del

Syntax: del <mac> <vid>

Description: Deletes a static MAC address entry.

Arguments:

<mac>: mac address, format: 00-02-03-04-05-06

<vid>: VLAN ID, range from 0-4094. VID must be 0 if VLAN mode is not tag-based.

Example:

```
SS2GD8I(mac-table-static-mac)# del 00-02-03-04-05-06 0
```

show filter

Syntax: show filter

Description: Displays the static filter table.

Arguments: None

Example:

```
SS2GD8I(mac-table-static-mac)# show filter
Static Filtering Etnry: (Total 1 item(s))
1) mac: 00-33-03-04-05-06, vid: -, alias: ccc
```

show forward

Syntax: show forward

Description: Displays the static forwarding table.

Arguments: None

Example:

```
SS2GD8I(mac-table-static-mac)# show forward
Static Forwarding Etnry: (Total 1 item(s))
1) mac: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa
```

> management

delete

Syntax: delete # **Description:** To delete a specific record or range.

Arguments: <#>: a specific or range management security entry(s)

Possible values: None.

Example:

```
SS2GD8I(management)# show
#: 1
Name : Tom     VlanID : 2  IP : 192.168.1.30-192.168.1.80
Type : SNMP    Action : Deny     Port : 1,2
SS2GD8I(management)# delete 1
SS2GD8I(management)# show
Security rule list is empty now
```

>> add

set

Syntax: set name <name> [vid <vid>] [ip <ip>] [port <port>] [type <type>] action <action>

Description: Allows a user to manage the switch using one or more methods and from one or more IP addresses and/or ports. If you just enter the command “set”, you will be prompted for each option.

Arguments:

name <name>: access control list (ACL) user name.

vid <vid> (optional): VLAN ID, range from 1-4095 or “any”, default is “any”.

ip <ip> (optional): IP range that user can log in from, or “any”, e.g. 192.168.1.90-192.168.1.90, default is “any”.

port <port> (optional): Physical port that user can log in from, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8, default is all ports.

type <type> (optional): Access type for user, can be “h” for HTTP, “s” for SNMP, “t” for Telnet, or “any”, or a combination of two of the three, separated by a comma, default is “any”.

action <action>: a(ccept) or d(eny).

Example:

```
SS2GD8I(management-add)# set name Mary vid 20 ip 192.168.1.1-192.168.1.90
port 2-5,8 type h,s action a
SS2GD8I(management-add)# show
#: 1
Name : Mary       VlanID : 20      IP : 192.168.1.1-192.168.1.90
Type : Http,SNMP  Action : Accept  Port : 2,3,4,5,8
```

>> edit

set

Syntax: set name <name> [vid <vid>] [ip <ip>] [port <port>] [type <type>] action <action> [<type> <value>] <action> <value>

Description: Edits a management policy record.

Arguments:

name <name>: access control list (ACL) user name.

vid <vid> (optional): VLAN ID, range from 1-4095 or “any”, default is “any”.

ip <ip> (optional): IP range that user can log in from, or “any”, e.g. 192.168.1.90-192.168.1.90, default is “any”.

port <port> (optional): Physical port that user can log in from, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8, default is all ports.

type <type> (optional): Access type for user, can be “h” for HTTP, “s” for SNMP, “t” for Telnet, or “any”, or a combination of two of the three, separated by a comma, default is “any”.

action <action>: a(ccept) or d(eny).

Example:

```
SS2GD8I(management)# edit 1
SS2GD8I(management-edit-1)# set name Tom vid 2 ip 192.168.1.30-
192.168.1.80 port 1-2 type s action d
SS2GD8I(management-edit-1)# show
#: 1
Name : Tom     VlanID : 2       IP : 192.168.1.30-192.168.1.80
Type : SNMP    Action : Deny    Port : 1,2
```

show

Syntax: show

Description: Shows all management policy records.

Arguments: None.

Example:

```
SS2GD8I(management)# show
#: 1
Name : Tom     VlanID : 2  IP : 192.168.1.30-192.168.1.80
Type : SNMP    Action : Deny     Port : 1,2
```

> max-pkt-len

set len

Syntax: set len <port range> <length>

Description: Sets the maximum length of the packet that each port can accept.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<length (bytes)>: maximum packet length, can be 1518, 1532, or 9208.

Example:

```
SS2GD8I(max-pkt-len)# set len 1-8 9208
```

show

Syntax: show

Description: Shows the current maximum packet length setting.

Arguments: None.

Example:

```
SS2GD8I(max-pkt-len)# show
PORT    Max Packet Length
------ ------------------
1       1532
2       1532
3       1532
4       1532
5       1532
6       1532
7       1532
8       1532
```

> mirror

set mirror-mode

Syntax: set mirror-mode <mode>

Description: Sets the mode of port mirroring.

Arguments:

<mode>: can be “rx” to enable mirroring or “disable” to disable it.

Example:

```
SS2GD8I(mirror)# set mirror-mode rx
```

set monitored-port

Syntax: set monitored-port <port range>

Description: Sets which port(s) will be monitored. Packets received by this port will be copied to the monitoring port.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(mirror)# set monitored-port 3-5,8
```

set monitoring-port

Syntax: set monitoring-port <#>

Description: Sets the port that will receive the mirrored packets. Administrators can view the packets that the monitored port(s) receives via this port.

Arguments:

<#>: the monitoring port. Only one port is allowed to configure, ranges from 1 to 8

Example:

```
SS2GD8I(mirror)# set monitoring-port 2
```

show

Syntax: show

Description: Displays the port mirroring settings.

Arguments: None.

Example:

```
SS2GD8I(mirror)# show
Mirror Mode : rx
Monitoring Port : 2
Monitored Port : 3 4 5 8
```

> port

clear counter

Syntax: clear counter

Description: Clears all ports’ counters (including simple and detail port counters).

Arguments: None.

Example:

```
SS2GD8I (port)# clear counter
```

disable flow-control

Syntax: disable flow-control <port range>

Description: Disables flow control for a port(s).

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I (port)# disable flow-control 6
```

disable state

Syntax: disable state <port range>

Description: Disables a port(s).

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I (port)# disable state 1-2
```

enable flow-control

Syntax: enable flow-control <range>

Description: Enable flow control for a port(s).

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I (port)# enable flow-control 3-8
```

enable state

Syntax: enable state <range>

Description: Enables a port(s).

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I (port)# enable state 3-7
```

set speed-duplex

Syntax: set speed-duplex <port range> <speed>

Description: Sets the speed and duplex of a port(s).

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<speed>: the speed of the port, can be any of the following:

auto - set auto-negotiation mode

10half - set speed/duplex 10M Half

10full - set speed/duplex 10M Full

100half - set speed/duplex 100M Half

100full - set speed/duplex 100M Full

1Gfull - set speed/duplex 1G Full

Example:

```
SS2GD8I(port)# set speed-duplex 5 auto
```

show conf

Syntax: show conf

Description: Displays each port’s state, speed-duplex and flow control.

Arguments: None.

Example:

```
SS2GD8I (port)# show conf
```

show detail-counter

Syntax: show detail-counter <#>

Description: Displays the detailed counter for each port.

Arguments:

<#>: port, range from 1 to 8

Example:

```
SS2GD8I (port)# show detail-counter 5
```

show sfp

Syntax: show sfp <port>

Description: Displays information on the SFP module.

Arguments:

<port>: SFP port, can be 7 or 8

Example:

```
SS2GD8I (port)# show sfp 7
Port 7 SFP information
------------------------------------------------------------
Connector Type         : SFP - LC
Fiber Type             : Multi-mode (MM)
Tx Central Wavelength  : 850
Baud Rate              : 1G
Vendor OUI             : 00:40:c7
Vendor Name            : APAC Opto
Vendor PN              : KM28-C3S-TC-N
Vendor Rev             : 0000
Vendor SN              : 5425010708
Date Code              : 050530
Temperature            : none
Vcc                    : none
Mon1 (Bias) mA         : none
Mon2 (TX PWR)          : none
Mon3 (RX PWR)          : none
```

show simple-counter

Syntax: show simple-counter

Description: Displays the simple counter for each port.

Arguments: None.

Example:

```
SS2GD8I (port)# show simple-counter
```

show status

Syntax: show status

Description: Displays the current status of the ports.

Arguments: None.

Example:

```
SS2GD8I (port)# show status
```

> qos

set advance-layer4

Syntax: set advance-layer4 <port-range> <#> <tcp/udp port> <default> <match>

Description: Sets the class of ports on advanced mode for Layer 4 QoS.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<#>: special UDP/TCP port selection, range from 1-10.

<tcp/udp port range>: TCP/UDB port, range from 0-65535.

<default>: default class (all other TCP/UDP ports), can be 1 (high) or 0 (low).

<match>: special TCP/UDP class, can be 1 (high) or 0 (low).

Example:

```
SS2GD8I(qos)# set advance-layer4 5 2 80 1 0
```

set default

Syntax: set default <class>

Description: Sets the priority class of the packets that QoS doesn’t affect.

Arguments:

<class>: class of service, can be 1 (high) or 0 (low).

Example:

```
SS2GD8I(qos)# set default 1
```

set diffserv

Syntax: set diffserv <ds-range> <class>

Description: Sets class of ports for IP DiffServ QoS.

Arguments:

<ds-range>: DSCP field, can be a single number (e.g. “1”) or a range of numbers (e.g. “5-7”), range from 0-63.

<class>: class of service, can be 1 (high) or 0 (low).

Example:

```
SS2GD8I(qos)# set diffserv 0-20 1
```

set mode

Syntax: set mode <mode>

Description: Sets QoS priority mode of the switch.

Arguments:

<mode>: can be “port” for per port priority, “pri_tag” for VLAN tag priority, “tos” for IP ToS classification, “layer4” for IP TCP/UDP port classification, or “diffserv” for IP DiffServ classification

Example:

```
SS2GD8I(qos)# set mode port
```

set port

Syntax: set port <port range> <class>

Description: Sets the class of ports for on port-based QoS

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<class>: class of service, can be 1 (high) or 0 (low).

Example:

```
SS2GD8I(qos)# set port 1-8 1
```

set pri-tag

Syntax: set pri_tag <port-range> <tag-range> <class>

Description: Sets class of ports on VLAN tag-based QoS.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<tag-range>: tag priority level, can be a single level (e.g. “1”) or a range of levels (e.g. “5-7”), range from 0-7.

<class>: class of service, can be 1 (high) or 0 (low).

Example:

```
SS2GD8I(qos)# set pri-tag 1-7 1-2 1
```

set simple-layer4

Syntax: set simple-layer4 <#>

Description: Sets class of ports on simple mode of Layer 4 QoS.

Arguments:

<#>: layer-4 configuration mode, valid values are:

0 - disable IP tcp/udp port classification

1 - lower priority of web browsing, e-mail, FTP and news

2 - prioritize IP telephony (VoIP)

3 - prioritize iSCSI

4 - prioritize web browsing, e-mail, FTP transfers and news

5 - prioritize streaming Audio/Video

6 - prioritize databases (Oracle, IBM DB2, SQL, Microsoft)

Example:

```
SS2GD8I(qos)# set simple-layer4 2
```

set tos

Syntax: set tos <port-range> <tos-range> <class>

Description: Sets the class of ports for IP ToS QoS.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<tos-range>: ToS precedence field, can be a single number (e.g. “1”) or a range of numbers (e.g. “5-7”), range from 0-7.

<class>: class of service, can be 1 (high) or 0 (low).

Example:

```
SS2GD8I(qos)# set tos 1-5 0-3 0
```

show

Syntax: show

Description: Displays the information of the active QoS mode.

Arguments: None.

Example:

```
SS2GD8I (qos)# show
IP Diffserv Classification
Default Class:high
DiffServ Class DiffServ Class DiffServ Class DiffServ Class
-------- ----- -------- ----- -------- ----- -------- -----
   0      high    1      high    2      high    3      high
   4      high    5      high    6      high    7      high
   8      high    9      high    10     high    11     high
   12     high    13     high    14     high    15     high
   16     high    17     high    18     high    19     high
   20     high    21     high    22     high    23     high
   24     high    25     high    26     high    27     high
   28     high    29     high    30     high    31     high
   32     high    33     high    34     high    35     high
   36     high    37     high    38     high    39     high
   40     high    41     high    42     high    43     high
   44     high    45     high    46     high    47     high
   48     high    49     high    50     high    51     high
   52     high    53     high    54     high    55     high
   56     high    57     high    58     high    59     high
   60     high    61     high    62     high    63     high
```

> reboot

reboot

Syntax: reboot

Description: Reboots the switch.

Arguments: None.

Example:

```
SS2GD8I# reboot
```

> snmp

disable

Syntax: disable <type>

Description: Disables SNMP or set-community.

Arguments:

<type>: Can be “snmp” or “set-community”.

Example:

```
SS2GD8I(snmp)# disable snmp
SS2GD8I(snmp)# disable set-community
```

enable

Syntax: enable <type>

Description: Enables SNMP or set-community.

Arguments:

<type>: Can be “snmp” or “set-community”.

Example:

```
SS2GD8I(snmp)# enable snmp
SS2GD8I(snmp)# enable set-community
```

set

Syntax:

set get-community <community>

set set-community <community>

set trap <#> <ip> [port] [community]

Description: Sets the community used for get-community or set-community, or sets the trap host IP, host port and trap-community.

Arguments:

<#>: trap number, range from 1-6.

<ip>: IP address or domain name.

<port>: trap port, range from 1-65535.

<community>:trap community name.

Example:

```
SS2GD8I(snmp)# set get-community public
SS2GD8I(snmp)# set set-community private
SS2GD8I(snmp)# set trap 1 192.168.1.1 162 public
```

show

Syntax: show

Description: Displays the SNMP configuration.

Arguments: None.

Example:

```
SS2GD8I(snmp)# show
SNMP     : Enable
Get Community: public
Set Community: private [Enable]
Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community: public
Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community: public
Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community: public
```

> stp

MCheck

Syntax: MCheck <port range>

Description: Forces the port to transmit RST BPDUs.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(stp)# Mcheck 1-8
```

disable

Syntax: disable

Description: Disables STP.

Possible values: None.

Example:

```
SS2GD8I(stp)# disable
```

enable

Syntax: enable

Description: Enables STP.

Arguments: None.

Example:

```
SS2GD8I(stp)# enable
```

set config

Syntax: set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

Description: Set the STP parameters.

Arguments:

<Bridge Priority>: priority must be a multiple of 4096, range from 0 to 61440.

<Hello Time>: range from 1 to 10.

<Max. Age>: range from 6 to 40.

<Forward Delay>: range from 4 to 30. Note: 2*(Forward Delay -1) >= Max Age, Max Age >= 2*(Hello Time +1)

Example:

```
SS2GD8I(stp)# set config 61440 2 20 15
```

set port

Syntax: set port <port range> <path cost> <priority> <edge_port> <admin p2p>

Description: Sets the STP port information.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<path cost>: range from 0-200000000. 0 means auto status.

<priority>: priority must be a multiple of 16, range from 0 to 240.

<edge_port>: admin edge port, can be “yes” or “no”.

<admin p2p>: admin point to point, can be “auto”, “|true”, or “false”.

Example:

```
SS2GD8I(stp)# set port 1-8 0 128 yes auto
```

set version

Syntax: set version <ver>

Description: Set the STP version.

Arguments:

<ver>: can be “stp” or “rstp”.

Example:

```
SS2GD8I(stp)# set version rstp
```

show config

Syntax: show config

Description: Displays the STP configuration.

Arguments: None

Example:

```
SS2GD8I(stp)# show config
STP State Configuration    :
Spanning Tree Protocol     : Enabled
Bridge Priority (0-61440)  : 61440
Hello Time (1-10 sec)      : 2
Max. Age (6-40 sec)        : 20
Forward Delay (4-30 sec)   : 15
Force Version              : RSTP
```

show port

Syntax: show port

Description: Displays the STP port information.

Arguments: None.

Example:

```
SS2GD8I# stp
SS2GD8I(stp)# show port
Port Port Status Path Cost Priority Admin Edge Port Admin Point To Point
==== =========== ========= ======== =============== ====================
1    DISCARDING  2000000    128         No                Auto
2    DISCARDING  2000000    128         No                Auto
3    DISCARDING  2000000    128         No                Auto
4    DISCARDING  2000000    128         No                Auto
5    DISCARDING  2000000    128         No                Auto
6    DISCARDING  2000000    128         No                Auto
7    DISCARDING  2000000    128         No                Auto
8    DISCARDING  2000000    128         No                Auto
```

show status

Syntax: show status

Description: Displays the STP status.

Arguments: None.

Example:

```
SS2GD8I(stp)# show status
STP Status :
STP State                              : Enabled
Bridge ID                              : 00:40:C7:D8:09:1D
Bridge Priority                        : 61440
Designated Root                        : 00:40:C7:D8:09:1D
Designated Priority                    : 61440
Root Port                              : 0
Root Path Cost                         : 0
Current Max. Age(sec)                  : 20
Current Forward Delay(sec)             : 15
Hello Time(sec)                        : 2
STP Topology Change Count              : 0
Time Since Last Topology Change(sec)   : 848
```

> system

set contact

Syntax: set contact <contact>

Description: Sets the contact description for the switch.

Arguments:

<contact>: a string of up to 40 characters.

Example:

```
SS2GD8I(system)# set contact networkadmin
```

set device-name

Syntax: set device-name <device-name>

Description: Sets the device name description for the switch.

Arguments:

<device-name>: a string of up to 40 characters.

Example:

```
SS2GD8I(system)# set device-name CR-2600
```

set location

Syntax: set location <location string>

Description: Sets the location description for the switch.

Arguments:

<location>: a string of up to 40 characters.

Example:

```
SS2GD8I(system)# set location HQ
```

show

Syntax: show

Description: Displays the basic information for the switch.

Arguments: None

Example:

```
SS2GD8I(system)# show
Model Name                    : SS2GD8I
System Description            : L2 Managed Switch
Location                      : HQ
Contact                       : networkadmin
Device Name                   : SS2GD8I
System Up Time                : 0 Days 3 Hours 28 Mins 17 Secs
Current Time                  : Sat Jan 1 14:37:19 2005
BIOS Version                  : v1.01
Firmware Version              : v2.14
Hardware-Mechanical Version   : v1.01-v1.01
Serial Number                 : 030F03000003
Host IP Address               : 192.168.1.1
Host MAC Address              : 00-40-c7-de-00-e7
Device Port                   : UART * 1, TP * 6, Dual-Media
                                Port(RJ45/SFP) * 2
RAM Size                      : 16 M
Flash Size                    : 2 M
```

> tftp

set server

Syntax: set server <ip>

Description: Sets the IP address of the TFTP server.

Arguments:

<ip>: the IP address of tftp server

Example:

```
SS2GD8I(tftp)# set server 192.168.3.111
```

show

Syntax: show

Description: Display the information of the TFTP server.

Arguments: None.

Example:

```
SS2GD8I(tftp)# show
Tftp Server : 192.168.3.111
```

> time

set daylightsaving

Syntax: set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>

Description: Sets the daylight saving time.

Arguments:

<hr>: daylight saving hour differential, range: -5 to +5

<MM/DD/HH>: daylight saving start month (01-12), day (01-31), and hour (00-23)

<mm/dd/hh>: daylight saving end month (01-12), day (01-31), and hour (00-23)

Example:

```
SS2GD8I(time)# set daylightsaving 3 10/12/01 11/12/01
Save Successfully
```

set manual

Syntax: set manual <YYYY/MM/DD> <hh:mm:ss>

Description: Sets the current time manually.

Arguments:

<YYYY/MM/DD>: year (2000-2036), month (01-12), and day (01-31)

<hh:mm:ss>: hour (00-23), minute (00-59), and second (00-59)

Example:

```
SS2GD8I(time)# set manual 2004/12/23 16:18:00
```

set ntp

Syntax: set ntp <ip> <timezone>

Description: Sets the current time via an NTP server.

Arguments:

<ip>: IP address or domain name of NTP server.

<timezone>: time zone (GMT), range from -12 to +13

Example:

```
SS2GD8I(time)# set ntp clock.via.net -5
Synchronizing...(1) Synchronization success
```

show

Syntax: show

Description: Shows the time settings.

Arguments: None.

Possible values: None.

Example:

```
SS2GD8I(time)# show
Current Time            : Thu Thu 14 15:04:03 2005
NTP Server              : 209.81.9.7
Timezone                : GMT+8:00
Day light Saving        : 0 Hours
Day light Saving Start  : Mth: 1 Day: 1 Hour: 0
Day light Saving End    : Mth: 1 Day: 1 Hour: 0
```

> trunk

del trunk

Syntax: del trunk <port range>

Description: Deletes a trunk.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(trunk)# del trunk 1
```

set priority

Syntax: set priority <range>

Description: Sets the LACP system priority.

Arguments:

<range>: available from 1 to 65535.

Example:

```
SS2GD8I(trunk)# set priority 33333
```

set trunk

Syntax: set trunk <port-range> <method> <group> <active LACP>

Description: Sets up a trunk, including the group number, mode, and LACP mode.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<method>: can be “static” to adopt the static link aggregation or “lacp” to adopt a dynamic link aggregation using link aggregation control protocol.

<group>: range from 1-8.

<active LACP>: can be “active” to set the LACP to active mode or “passive” to set the LACP to passive mode

Example:

```
SS2GD8I(trunk)# set trunk 1-4 lacp 1 active
```

show aggtr-view

Syntax: show aggtr-view

Description: Displays the aggregator list.

Arguments: None

Example:

```
SS2GD8I(trunk)# show aggtr-view
Aggregator 1) Method: None
              Member Ports: 1
              Ready Ports: 1
Aggregator 2) Method: LACP
              Member Ports: 2
              Ready Ports:
```

show lacp-detail

Syntax: show lacp-detail <aggtr>

Description: Displays detailed information for the LACP trunk group.

Arguments:

<aggtr>: aggregator, range from 1 to 8

Example:

```
SS2GD8I(trunk)# show lacp-detail 2
Aggregator 2 Information:
             Actor                            Partner
--------------------------------- -----------------------------
System Priority     MAC Address    System Priority   MAC Address
--------------- ----------------- --------------- -------------
     32768      00-40-c7-e8-00-02       32768   00-00-00-00-00-00
 Port     Key       Trunk Status           Port            Key
------ -------- ----------------- --------------- -------------
  2      257           ---                2              0
```

show lacp-priority

Syntax: show lacp-priority

Description: Displays the LACP Priority.

Arguments: None

Example:

```
SS2GD8I(trunk)# show lacp-priority
LACP System Priority : 32768
```

show status

Syntax: show status

Description: Displays the aggregator status and settings for each port.

Arguments: None.

Example:

```
SS2GD8I(trunk)# show status
         Trunk Port Setting              Trunk Port Status
------------------------------------ ----------------------
 Port   Method    Group   Active LACP   Aggregator    Status
====== ======== ======= ============= ============= ========
  1      None       0       Active           1          ---
  2      None       0       Active           2          ---
  3      LACP       2       Active           3          ---
  4      None       0       Active           4          ---
  5      None       0       Active           5          ---
  6      None       0       Active           6          ---
  7      None       0       Active           7          ---
  8      None       0       Active           8          ---
```

> vlan

del port-group

Syntax: del port-group <name>

Description: Deletes a port-based VLAN group.

Arguments:

<name>: the VLAN group to delete.

Example:

```
SS2GD8I(vlan)# del port-group VLAN-2
```

del tag-group

Syntax: del tag-group <vid>

Description: Delete a tag-based VLAN group.

Arguments:

<vid>: the VLAN group to delete, range from 1 to 4094

Example:

```
SS2GD8I(vlan)# del tag-group 2
```

disable drop-untag

Syntax: disable drop-untag <port range>

Description: Disables dropping of untagged frames.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Possible values: <range>: 1 to 8

Example:

```
SS2GD8I(vlan)# disable drop-untag 5-8
```

disable sym-vlan

Syntax: disable sym-vlan <port range>

Description: Disables dropping of frames from non-member port(s).

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(vlan)# disable sym-vlan 5-8
```

enable drop-untag

Syntax: enable drop-untag <port range>

Description: Drops untagged frames.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(vlan)# enable drop-untag 5-8
```

enable sym-vlan

Syntax: enable sym-vlan <range>

Description: Enabled dropping of frames from non-member port(s).

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(vlan)# enable sym-vlan 5-8
```

set mode

Syntax: set mode <mode> [up-link]

Description: Switches VLAN mode.

Arguments:

<mode>: can be “disable” to disable VLANs, “tag” to set tag-based VLAN, “port” to set port-based VLAN, “metro” to set metro mode VLAN, or “double-tag” to enable Q-in-Q function.

[up-link] (optional): can be “7”, “8”, or “7,8”, only for metro mode VLAN

Example:

```
SS2GD8I(vlan)# set mode port
```

set port-group

Syntax: set port-group <name> <port range>

Description: Adds or edits a port-based VLAN group.

Arguments:

<name>: port-VLAN name

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

Example:

```
SS2GD8I(vlan)# set port-group VLAN-1 2-5,6,8
```

set port-role

Syntax: set port-role <port range> <role> [vid]

Description: Sets egress rule and configures port roles.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<role>: can be “access” to not tag frames, “trunk” to tag all frames, or “hybrid” to tag all frames except a specific VID.

[vid] (optional): untag-VID for hybrid port, range from 1-4094.

Example:

```
SS2GD8I(vlan)# set port-role 5 hybrid 6
```

set pvid

Syntax: set pvid <port range> <pvid>

Description: Sets the PVID of VLANs.

Arguments:

<port range>: which ports to change, can be a single port (e.g. “1”) or a range of ports (e.g. “5-7”), range from 1-8.

<pvid>: which PVID(s) to set, from from 1 to 4094

Example:

```
SS2GD8I(vlan)# set pvid 3,5,6-8 5
```

set tag-group

Syntax: set tag-group <vid> <name> <range> <#>

Description: Adds or edits a tag-based VLAN group.

Arguments:

<vid>: VLANID, range from 1 to 4094.

<name>: tag-VLAN name.

<range>: VLAN group members, can be a single number (e.g. “1”) or a range of numbers (e.g. “5-7”), range from 1-8.

<#>: Can be 1 for symmetric VLAN or 0 for asymmetric VLAN.

Example:

```
SS2GD8I(vlan)# set tag-group 2 VLAN-2 2-5,6,8 0
```

show group

Syntax: show group

Description: Displays the VLAN mode and groups.

Arguments: None.

Possible values: None.

Example:

```
SS2GD8I(vlan)# show group
Vlan mode is double-tag.
1) Vlan Name   : default
   Vlan ID     : 1
   Sym-vlan    : Disable
   Member      : 1 2 3 4 5 6 7    8
2) Vlan Name   : VLAN-2
   Vlan ID     : 2
   Sym-vlan    : Disable
   Member      : 2 3 4 5 6
```

show pvid

Syntax: show pvid

Description: Displays pvid and ingress/egress rules.

Arguments: None.

Example:

```
SS2GD8I(vlan)# show pvid
 Port    PVID    Rule1      Rule2    Port Rule   Untag Vid
------ ------ --------- --------- ----------- -----------
  1       1    Disable   Disable     Access        -
  2       1    Disable   Disable     Access        -
  3       5    Disable   Disable     Access        -
  4       1    Disable   Disable     Access        -
  5       5    Enable    Disable     Hybrid        6
  6       5    Enable    Disable     Access        -
  7       5    Enable    Disable     Access        -
  8       5    Enable    Disable     Access        -
```

> vs

disable

Syntax: disable

Description: Disables the virtual stack.

Arguments: None.

Example:

```
SS2GD8I(vs)# disable
```

enable

Syntax: enable

Description: Enables the virtual stack.

Arguments: None.

Possible values: None.

Example:

```
SS2GD8I(vs)# enable
```

set gid

Syntax: set gid <gid>

Description: Sets the group ID.

Arguments:

<gid>:Group ID

Example:

```
SS2GD8I(vs)# set gid group1
```

set role

Syntax: set role <role>

Description: Sets the role.

Arguments:

<role>: can be “master” to act as master or “slave” to act as slave.

Example:

```
SS2GD8I(vs)# set role master
```

show

Syntax: show

Description: Displays the configuration of the virtual stack.

Arguments: None.

Example:

```
SS2GD8I(vs)# show
Virtual Stack Config:
State    : Enable
Role     : Master
Group ID : group1
```

5 Troubleshooting

5.1 Resolving Connection Problems

Possible causes a connection problem where the Link LED does not light up even though the cable is connect are:

- The attached device is not powered on.
- The cable may not be the correct type or is defective.
- The cable installed in the building is defective.
- The connection has come loose on either end.
- The port is defective.

5.2 Q&A

Q1. Computer A can connect to Computer B, but cannot connect to Computer C through the switch.

A1. There are many possibilities for this issue, including:

- The network device on Computer C may be defective. Check the Link/Act status of the port connected to Computer C on the switch. Try connecting Computer C to another port, and try another connecting another device to this port to ensure the port is not defective.
- The network configuration on Computer C may be incorrect. Verify that the network settings (e.g. IP address, subnet mask) on Computer C are correct.
- A software firewall on Computer C (e.g. ZoneAlarm, Windows Firewall, Norton Firewall) is preventing access to the computer.
- Computer A and Computer C are set up on separate VLANs on the switch and therefore cannot communicate with each other.

Q2. User is unable to access the CLI through the console port.

A2. Check the following:

- The COM port default parameters are [Baud Rate: 57600, Data Bits: 8, Parity Bits: None, Stop Bit: A, Flow Control: None]. Verify the COM port parameters in the terminal program.
- Check the RS-232 cable is not damaged and is connected properly into the console port on the switch and the serial port of the computer.
- Check if the COM of the PC is enabled.

Appendix A: Technical Specifications

Features

- 6 (10/100/1000Mbps) Gigabit Ethernet ports that are compliant with IEEE802.3, 802.3u, 802.3z and 802.3ab.
- 2 Gigabit Combo-SFP copper/fiber ports dual media ports automatically detect which cable is connected.
- Non-blocking store-and-forward shared-memory switch.
- Supports auto-negotiation for configuring speed and duplex mode.
- Supports 802.3x flow control for full-duplex ports.
- Supports collision-based and carrier-based backpressure for half-duplex ports.
- Any ports can be set to disabled mode, force mode or auto-polling mode.
- Supports Head of Line (HOL) blocking prevention.
- Supports broadcast storm filtering.
- Auto-aging with programmable inter-age time.
- Supports 802.1p Class of Service with 2-level priority queuing.
- Supports port sniffing
- Programmable maximum Ethernet frame length from 1518 to 9208 bytes (jumbo frames).
- Supports port-based VLAN and 802.1Q tag-based VLAN.
- Efficient self-learning and address recognition mechanism enables forwarding rate at wire speed.
- Supports management using a single IP address for easy management.
- Web-based management provides the ability to manage the switch from any web browser.
- SNMP/Telnet interface allows for in-band management.
- Supports IEEE 802.1d Spanning Tree Protocol.
- Supports IEEE 802.1w Rapid Spanning Trees.
- Supports IEEE 802.1X port-based network access control.
- Supports IP Multicasting to implement IGMP Snooping function.
- Supports 802.1p Class of Service with 2-level priority queuing.
- Supports 802.3ad port trunking with flexible load distribution and failover.
- Supports ingress port security mode for VLAN Tagged and Untagged frames.
- Supports SNMP MIB2 and RMON sampling with sampled packet error indication.

Hardware Specifications

- Standard Compliance: IEEE 802.3 / 802.3ab / 802.3z / 802.3u / 802.3x.
- Network Interface: gigabit copper and gigabit fiber using SFP transceivers.
- Ports 7 and 8 are Combo-SFP dual media ports with auto detection.
- SFP module supports LC and BiDi LC transceivers.

- Transmission Mode: 10/100Mbps supports full or half duplex, 1000Mbps supports full duplex only
- Transmission Speed: 10/100/1000Mbps for Copper, 1000Mbps for Fiber
- Full Forwarding/Filtering Packet Rate: PPS (packets per second)

Forwarding Rate	Speed
1,488,000 PPS	1000 Mbps
148,800 PPS	100 Mbps
14,880 PPS	10 Mbps

- MAC Address and Self-learning: 8K MAC address, 4K VLAN table entries
- Buffer Memory: Embedded 144 KB frame buffer
- Flow Control: IEEE802.3x compliant for full duplex, Backpressure flow control for half duplex
- Maximum Cable Lengths:

Copper	Cat. 5 UTP cable, up to 100m
1000Base-SX	Up to 220/275/500/550m, depending on Multi-Mode Fiber type
1000Base-LX	Single-Mode Fiber, up to10/30/50km
1000Base-LX WDM (BiDi)	Single-Mode Fiber, up to 20km

- Diagnostic LEDs:
  - System LEDs: Power, CPU
  - Copper Ports 1 to 8: LINK/ACT, 10/100/1000Mbps
  - SFP Fiber Ports 7 & 8: SFP(LINK/ACT)
- Power Requirement: AC Line
  - Voltage: 100-240 V
  - Frequency: 50-60 Hz
  - Consumption: 13W
- Ambient Temperature: 32 to 104°F (0 to 40°C)
- Humidity: 5% to 90%
- Dimensions (H x W x D): 1.7 x 8.7 x 5.1 in (44 x 220 x 130.5 mm)
- Complies with FCC Part 15 Class A & CE Mark Approval